

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 3 日
Date of Application:

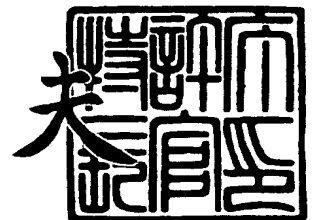
出 願 番 号 特 願 2 0 0 2 - 3 5 1 0 6 3
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 5 1 0 6 3]

出 願 人 松 下 電 器 産 業 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 1 1 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 9 1 0 8 8

【書類名】 特許願

【整理番号】 2022540497

【提出日】 平成14年12月 3日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32
G09C 1/00 640

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山道 将人

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 館林 誠

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 暗号システム、暗号装置、復号装置、共有鍵生成装置及び共有鍵復元装置

【特許請求の範囲】

【請求項 1】 共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第 1 の暗号化手段とを備えることを特徴とする、共有鍵生成装置。

【請求項 2】 共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第 1 の暗号予備データを生成する第 1 の暗号化手段と、

前記秘密数データを前記検証値データに基づいて暗号化して第 2 の暗号予備データを生成する第 2 の暗号化手段とを備え、

前記暗号化共有鍵データは、前記第 1 の暗号予備データと前記第 2 の暗号予備データから構成されることを特徴とする、共有鍵生成装置。

【請求項 3】 前記第 2 の暗号化手段は、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第 2 の暗号予備データを生成することを特徴とする、請求項 2 に記載の共有鍵生成装置。

【請求項 4】 前記第 2 の暗号化手段は、前記秘密数データを、前記検証値デ

ータを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第2の暗号予備データを生成することを特徴とする、請求項2に記載の共有鍵生成装置。

【請求項5】 前記第2の暗号化手段は、前記秘密数データに前記検証値データを加算して前記第2の暗号予備データを生成することを特徴とする、請求項2に記載の共有鍵生成装置。

【請求項6】 前記第2の暗号化手段は、前記秘密数データに前記検証値データを乗算して前記第2の暗号予備データを生成することを特徴とする、請求項2に記載の共有鍵生成装置。

【請求項7】 前記暗号化共有鍵データは、前記第1の暗号予備データと前記第2暗号予備データのビット連結データであることを特徴とする、請求項2から請求項6のいずれか一項に記載の共有鍵生成装置。

【請求項8】 前記第1の暗号化手段は、NTRU暗号方式により暗号化して前記暗号化共有鍵データを生成することを特徴とする、請求項1に記載の共有鍵生成装置。

【請求項9】 前記第1の暗号化手段は、NTRU暗号方式により暗号化して前記第1の暗号予備データを生成することを特徴とする、請求項2から請求項7のいずれか一項に記載の共有鍵生成装置。

【請求項10】 前記秘密数データは、ランダムに生成される乱数であることを特徴とする、請求項1から請求項9のいずれか一項に記載の共有鍵生成装置。

【請求項11】 前記共有鍵導出手段は、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする、請求項1から請求項10のいずれか一項に記載の共有鍵生成装置。

【請求項12】 予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第3の暗号化手段とを備え、

前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項13】 予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化手段と、

前記第2の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第2の復号化手段と、

前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化手段とを備え、

前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項14】 予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、

前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第1の復号化手段と、

前記第2の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第2の復号化手段と、

前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、

前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化手段とを備え、

前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前

記共有鍵データを出力することを特徴とする、共有鍵復元装置。

【請求項 15】 前記第 2 の復号化手段は、前記第 2 の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成することを特徴とする、請求項 13 または請求項 14 に記載の共有鍵復元装置。

【請求項 16】 前記第 2 の復号化手段は、前記第 2 の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成することを特徴とする、請求項 13 または請求項 14 に記載の共有鍵復元装置。

【請求項 17】 前記第 2 の復号化手段は、前記第 2 の暗号予備データに前記検証値データを減算して前記秘密数データを生成することを特徴とする、請求項 13 または請求項 14 に記載の共有鍵復元装置。

【請求項 18】 前記第 2 の暗号化手段は、前記第 2 の暗号予備データを前記検証値データで除算して前記秘密数データ第 2 の秘密数データを生成することを特徴とする、請求項 13 または請求項 14 に記載の共有鍵復元装置。

【請求項 19】 前記第 1 の復号化手段は、NTRU 暗号方式により復号化して前記共有鍵データを生成することを特徴とする、請求項 12 に記載の共有鍵復元装置。

【請求項 20】 前記第 1 の復号化手段は、NTRU 暗号方式により復号化して前記検証値データを生成することを特徴とする、請求項 13 から請求項 18 のいずれか一項に記載の共有鍵復元装置。

【請求項 21】 前記共有鍵導出手段は、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする、請求項 15 から請求項 20 のいずれか一項に記載の共有鍵復元装置。

【請求項 22】 予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して

第1の暗号予備データを生成する第1の暗号化手段と、

前記平文データを前記共有鍵データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化手段とを備え、

前記暗号文データは、前記第1の暗号予備データと前記第2の暗号予備データから構成されることを特徴とする、暗号装置。

【請求項23】 予め与えられた秘密鍵データ及び公開鍵データに基づいて、第1の暗号予備データと第2の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、

前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化手段とを備え、

前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記第2の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする、復号装置。

【請求項24】 予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵データ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムであって、

前記暗号装置は、

秘密数データを生成する秘密数データ生成手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化手段と、

前記平文データを前記共有鍵データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化手段とを備え、

前記暗号文データは、前記第 1 の暗号予備データと前記第 2 の暗号予備データと前記第 3 の暗号予備データから構成され、

前記復号装置は、

前記第 1 の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第 1 の復号化手段と、

前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、

前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第 3 の暗号予備データを生成する第 3 の暗号化手段とを備え、

前記第 1 の暗号予備データと前記第 3 の暗号予備データが一致する場合に、前記第 2 の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする、暗号システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、公開鍵暗号を用いた鍵配送に関するものである。

【 0 0 0 2 】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献 1 参照。）。この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータ内容を上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信内容データを受信する。そして、受信装置

は、暗号化された通信内容データを、自身の有する秘密鍵で復号して元の通信内容データを得る。

【0003】

1996年、高速処理が可能な公開鍵暗号として、NTRU暗号が提案された（例えば、非特許文献2参照。）。このNTRU暗号については、非特許文献2に詳細が記載されているのでここでは詳細な説明を省略するが、べき乗演算を行うRSA暗号や楕円曲線上の点のスカラ倍演算を行う楕円曲線暗号に比べ、高速に演算可能な多項式演算で暗号化と復号化を行うので、従来の公開鍵暗号よりもソフトウェアにより高速に処理することが可能である。なお、このNTRU暗号方式は、公開鍵を用いて平文を暗号化して暗号文を生成し、正規の秘密鍵を用いて暗号文を復号して復号文を生成しても、復号文が元の平文と異なる場合が発生する。このことを復号エラーが発生するという。なお、復号エラーを回避する方法として、平文に付加情報を付加して暗号化し、平文のハッシュ関数値と共に送信する方法が開示されている（例えば、特許文献1参照。）。

【0004】

一方で、近年、公開鍵暗号の新しい概念として、鍵カプセル化メカニズム（Key Encapsulation Mechanisms）と呼ばれる方式が提案された（例えば、非特許文献3参照。）。この鍵カプセル化メカニズムは、簡単に説明すると、公開鍵暗号を用いて送信装置と受信装置の間で共有鍵を配送するアルゴリズムであり、送信側が、暗号化アルゴリズムEに受信者の公開鍵 p_k を入力して暗号文Cと共有鍵Kを生成し、暗号文Cを受信側に伝送する。そして、受信側が、復号アルゴリズムDに、秘密鍵 s_k と暗号文Cを入力して送信側と同じ共有鍵Kを求める方式である。この鍵カプセル化メカニズムの目的は、鍵カプセル化メカニズムで共有鍵Kを送信装置と受信装置で共有することにより、その後、送信装置から受信装置へ通信される通信内容データを、共有鍵Kを用いて共通鍵暗号で暗号化することにある。ここで、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来にない特長である。

【0005】

このような鍵カプセル化メカニズムとして、RSA-KEMと呼ばれるアルゴリズムが開示されている（例えば、非特許文献3参照。）。以下に、この非特許文献3に記載されているRSA-KEMアルゴリズムについて説明する。

【0006】

(1) RSA-KEMのシステムパラメータ

RSA-KEMは、以下のシステムパラメータを持つ。

【0007】

・ハッシュ関数：G

なお、ハッシュ関数については、非特許文献1に詳細が記述されているので、ここでは説明を省略する。

【0008】

(2) RSA-KEMの公開鍵と秘密鍵

・素数 p 、 q を選び、 $n = p \cdot q$ を生成する。

【0009】

・ $(p-1)$ と $(q-1)$ の最小公倍数を計算し、 L とする。

【0010】

・ランダムに、 L と互いに素である Z_L の要素 e を選び、 $d = 1/e \bmod L$ を計算する。

【0011】

ここで、 Z_L は、 $\{0, 1, 2, \dots, L-1\}$ からなる集合である。

【0012】

・公開鍵 pk を (e, n) とし、秘密鍵 sk を (d, n) とする。

【0013】

(3) RSA-KEMの暗号化

暗号化時には、以下に述べる暗号化アルゴリズム $KemE$ に公開鍵 pk を入力して共有鍵 K と暗号文 C を出力する。以下に暗号化アルゴリズム $KemE$ について説明する。

【0014】

・ Z_n の要素 s をランダムに生成する。

【0015】

ここで、 Z_n は、 $\{0, 1, 2, \dots, n-1\}$ からなる集合である。

【0016】

- ・ $G(s)$ を生成し、 $K = G(s)$ とする。

【0017】

- ・ $C = s^e \bmod n$ を生成する。ここで「 \wedge 」はべき乗を表す。

【0018】

- ・ 共有鍵 K と暗号文 C を出力する。

【0019】

(4) PSEC-KEMの復号化

復号化時には、以下に述べる復号アルゴリズム $KemD$ に暗号文 C と秘密鍵 s_k を入力して共有鍵 K を出力する。以下に復号アルゴリズム $KemD$ について説明する。

【0020】

- ・ $s = C^d \bmod n$ を生成する。

【0021】

- ・ $G(s)$ を生成し、 $K = G(s)$ とする。

【0022】

- ・ 共有鍵 K を出力する。

【0023】

この RSA-KEM アルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵 p_k を取得し、取得した公開鍵 p_k を前述の暗号化アルゴリズム $KemE$ に入力して共有鍵 K と暗号文 C を導出して、暗号文 C を受信装置へ送信する。そして、受信装置は、送信装置から暗号文 C を受信し、受信した暗号文 C と自身が有する秘密鍵 s_k を前述の復号アルゴリズム $KemD$ に入力して、送信装置が導出したものと等しい共有鍵 K を導出する。

【0024】

以下に、このことを詳細に説明する。

【0025】

今、RSA-KEMアルゴリズムは、暗号化アルゴリズム K_{emE} で、ランダムに生成した要素 s を公開鍵 p_k を用いて暗号化して暗号文 C を生成する。そして、復号アルゴリズム K_{emD} では、暗号文 C から秘密鍵 s_k を用いて復号化して、暗号化アルゴリズム K_{emE} において生成されたランダムな要素 s を求めることができる。従って、暗号化アルゴリズム K_{emE} と復号アルゴリズム K_{emD} は、ハッシュ関数 G に同じ s の値を入力することができ、同じ共有鍵 K を導出することができる。この結果、秘密鍵 s_k を有する受信装置は、送信装置が導出したものと同じ共有鍵 K を導出できることになる。

【0026】

一方で、秘密鍵 s_k を知らない他の受信装置は、たとえ公開鍵 p_k を取得して暗号文 C を受信したとしても、秘密鍵 s_k を知らないので C から s を求めることができず、送信装置が導出したものと同じ共有鍵 K を導出できない。

【0027】

よって、以上により、送信装置と受信装置とは、共有鍵 K を秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵 K を用いて共通鍵暗号で暗号化することができる。

【0028】

【特許文献1】

特開 2002-252611 号公報

【非特許文献1】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997.

【非特許文献2】

Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.

【非特許文献3】

Victor Shoup, "A proposal for an ISO standard for public k

ey encryption (version 2.1)”, [online]、2001年12月20日、[2002年9月29日検索]、インターネット<URL: http://shoup.net/papers/iso-2_1.pdf>

【0029】

【発明が解決しようとする課題】

上述したように、RSA-KEMアルゴリズムは、暗号文Cから秘密鍵を知らなければ導出できないランダムな要素sをハッシュ関数Gに入力して共有鍵Kを導出するようにしている。従って、秘密鍵を知らなければその共有鍵Kを導出できないようにしている。

【0030】

しかしながら、NTRU暗号は、鍵カプセル化メカニズムであるRSA-KEMアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生した場合、秘密鍵を用いてもランダムな要素sが正しく導出できないので、正しい共有鍵Kを導出ないという問題点がある。すなわち、高速処理が可能なNTRU暗号は、鍵カプセル化メカニズムであるRSA-KEMアルゴリズムを適用しても、送信装置と受信装置との間で異なる鍵が導出される場合があり、従って、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができない。

【0031】

また、特許文献1は、暗号における復号エラー発生検出技術であり、鍵カプセル化メカニズムについては言及されていない。

【0032】

そこで、本発明は上記の課題に鑑み、NTRU暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第1の目的とする。

【0033】

また、他の公開鍵暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第2の目的とする。

【 0 0 3 4 】**【課題を解決するための手段】**

請求項 1 における発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第 1 の暗号化手段とを備えることを特徴とする。

【 0 0 3 5 】

請求項 2 における発明は、共有鍵データと、予め与えられた公開鍵データに基づいて前記共有鍵データを暗号化した暗号化共有鍵データを出力する共有鍵生成装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて検証値データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第 1 の暗号予備データを生成する第 1 の暗号化手段と、前記秘密数データを前記検証値データに基づいて暗号化して第 2 の暗号予備データを生成する第 2 の暗号化手段とを備え、前記暗号化共有鍵データは、前記第 1 の暗号予備データと前記第 2 の暗号予備データから構成されることを特徴とする。

【 0 0 3 6 】

請求項 3 における発明は、請求項 2 に記載の共有鍵生成装置は、前記第 2 の暗号化手段が、前記秘密数データと前記検証値データの排他的論理和演算を行って前記第 2 の暗号予備データを生成することを特徴とする。

【 0 0 3 7 】

請求項 4 における発明は、請求項 2 に記載の共有鍵生成装置は、前記第 2 の暗号化手段が、前記秘密数データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により暗号化して前記第 2 の暗号予備データを生成することを特徴とする。

【0038】

請求項5における発明は、請求項2に記載の共有鍵生成装置は、前記第2の暗号化手段が、前記秘密数データに前記検証値データを加算して前記第2の暗号予備データを生成することを特徴とする。

【0039】

請求項6における発明は、請求項2に記載の共有鍵生成装置は、前記第2の暗号化手段が、前記秘密数データに前記検証値データを乗算して前記第2の暗号予備データを生成することを特徴とする。

【0040】

請求項7における発明は、請求項2から請求項6のいずれか一項に記載の共有鍵生成装置は、前記暗号化共有鍵データが、前記第1の暗号予備データと前記第2暗号予備データのビット連結データであることを特徴とする。

【0041】

請求項8における発明は、請求項1に記載の共有鍵生成装置は、前記第1の暗号化手段が、NTRU暗号方式により暗号化して前記暗号化共有鍵データを生成することを特徴とする。

【0042】

請求項9における発明は、請求項2から請求項7のいずれか一項に記載の共有鍵生成装置は、前記第1の暗号化手段が、NTRU暗号方式により暗号化して前記第1の暗号予備データを生成することを特徴とする。

【0043】

請求項10における発明は、請求項1から請求項9のいずれか一項に記載の共有鍵生成装置は、前記秘密数データが、ランダムに生成される乱数であることを特徴とする。

【0044】

請求項11における発明は、請求項1から請求項10のいずれか一項に記載の共有鍵生成装置は、前記共有鍵導出手段が、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする。

【0045】

請求項 12 における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記暗号化共有鍵データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第 1 の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して再暗号化共有鍵データを生成する第 3 の暗号化手段とを備え、前記暗号化共有鍵データと前記再暗号化共有鍵データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【0046】

請求項 13 における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第 1 の暗号予備データと第 2 の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第 1 の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第 1 の復号化手段と、前記第 2 の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第 2 の復号化手段と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記検証値検証データを前記公開鍵データと前記乱数データに基づいて暗号化して第 3 の暗号予備データを生成する第 3 の暗号化手段とを備え、前記第 1 の暗号予備データと前記第 3 の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【0047】

請求項 14 における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第 1 の暗号予備データと第 2 の暗号予備データから構成される暗号化共有鍵データを復号して共有鍵データを出力する共有鍵復元装置であって、前記第 1 の暗号予備データを前記秘密鍵データに基づいて復号化して検証値データを生成する第 1 の復号化手段と、前記第 2 の暗号予備データを前記検証値データに基づいて復号化して秘密数データを生成する第 2 の復号化手段と、前記秘密数データを所定の処理に基づいて検証値検証データと乱数データと前記共有鍵データ

に変換する共有鍵導出手段と、前記検証値データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化手段とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記共有鍵データを出力することを特徴とする。

【0048】

請求項15における発明は、請求項13または請求項14に記載の共有鍵復元装置は、前記第2の復号化手段が、前記第2の暗号予備データと前記検証値データの排他的論理和演算を行って前記秘密数データを生成することを特徴とする。

【0049】

請求項16における発明は、請求項13または請求項14に記載の共有鍵復元装置は、前記第2の復号化手段が、前記第2の暗号予備データを、前記検証値データを暗号鍵として用いて共通鍵暗号方式により復号化して前記秘密数データを生成することを特徴とする。

【0050】

請求項17における発明は、請求項13または請求項14に記載の共有鍵復元装置は、前記第2の復号化手段が、前記第2の暗号予備データに前記検証値データを減算して前記秘密数データを生成することを特徴とする。

【0051】

請求項18における発明は、請求項13または請求項14に記載の共有鍵復元装置は、前記第2の暗号化手段が、前記第2の暗号予備データを前記検証値データで除算して前記秘密数データ第2の秘密数データを生成することを特徴とする。

【0052】

請求項19における発明は、請求項12に記載の共有鍵復元装置は、前記第1の復号化手段が、NTRU暗号方式により復号化して前記共有鍵データを生成することを特徴とする。

【0053】

請求項20における発明は、請求項13から請求項18のいずれか一項に記載の共有鍵復元装置は、前記第1の復号化手段が、NTRU暗号方式により復号化

して前記検証値データを生成することを特徴とする。

【0054】

請求項 21 における発明は、請求項 15 から請求項 20 のいずれか一項に記載の共有鍵復元装置は、前記共有鍵導出手段が、所定の処理として、一方向性ハッシュ関数を用いることを特徴とする。

【0055】

請求項 22 における発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置であって、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第 1 の暗号予備データを生成する第 1 の暗号化手段と、記平文データを前記共有鍵データに基づいて暗号化して第 2 の暗号予備データを生成する第 2 の暗号化手段とを備え、前記暗号文データは、前記第 1 の暗号予備データと前記第 2 の暗号予備データから構成されることを特徴とする。

【0056】

請求項 23 における発明は、予め与えられた秘密鍵データ及び公開鍵データに基づいて、第 1 の暗号予備データと第 2 の暗号予備データから構成される暗号文データを復号して復号文データを出力する復号装置であって、前記第 1 の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第 1 の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第 3 の暗号予備データを生成する第 3 の暗号化手段とを備え、前記第 1 の暗号予備データと前記第 3 の暗号予備データが一致する場合に、前記第 2 の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする。

【0057】

請求項 24 における発明は、予め与えられた公開鍵データに基づいて平文データを暗号化した暗号文データを生成する暗号装置、及び予め与えられた秘密鍵デ

ータ及び公開鍵データに基づいて暗号文データを復号して復号文データを出力する復号装置からなる暗号システムであって、前記暗号装置は、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第1の暗号予備データを生成する第1の暗号化手段と、前記平文データを前記共有鍵データに基づいて暗号化して第2の暗号予備データを生成する第2の暗号化手段とを備え、前記暗号文データは、前記第1の暗号予備データと前記第2の暗号予備データと前記第3の暗号予備データから構成され、前記復号装置は、前記第1の暗号予備データを前記秘密鍵データに基づいて復号化して秘密数データを生成する第1の復号化手段と、前記秘密数データを所定の処理に基づいて乱数データと共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して第3の暗号予備データを生成する第3の暗号化手段とを備え、前記第1の暗号予備データと前記第3の暗号予備データが一致する場合に、前記第2の暗号予備データを前記共有鍵に基づいて復号化して前記復号文データを生成する復号手段とを備えることを特徴とする。

【0058】

【発明の実施の形態】

以下、本発明に係る暗号システムの実施の形態について、図面を用いて説明する。

【0059】

本発明に係る暗号システムは、公開鍵暗号方式の一例として、NTRU暗号方式を用いる。NTRU暗号方式は、多項式の演算で暗号化と復号化を行う公開鍵暗号方式である。このNTRU暗号方式、及びNTRU暗号方式の公開鍵、及び秘密鍵の生成方法については、非特許文献2に詳しく述べられているので、ここでは詳細な説明を省略するが、以下にNTRU暗号方式について簡単に説明する。

【0060】

(1) NTRU暗号方式のシステムパラメータ

NTRU暗号方式は、整数のシステムパラメータ、 N 、 p 、 q を持つ。上記文献には、システムパラメータの例として、 $(N, p, q) = (107, 3, 64)$ 、 $(N, p, q) = (167, 3, 128)$ 、 $(N, p, q) = (503, 3, 256)$ の3つの例が挙げられている。

【0061】

以降、本発明に係る暗号システムの実施の形態では、システムパラメータ N を $N=167$ とした場合の説明を行う。

【0062】

(2) NTRU暗号方式の多項式演算

NTRU暗号方式は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。まず、NTRU暗号方式で扱う多項式は、上記システムパラメータ N に対し、 $N-1$ 次元以下の多項式であり、例えば $N=5$ のとき、 $X^4 + X^3 + 1$ 等の多項式である。ここで、「 X^a 」は X の a 乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵 h 、秘密鍵 f 、平文 m 、乱数 r 、暗号文 c はいずれも、 $N-1$ 次元以下の多項式として表現される（以降、それぞれを公開鍵多項式 h 、秘密鍵多項式 f 、平文多項式 m 、乱数多項式 r 、暗号文多項式 c と呼ぶ）。

【0063】

そして、多項式演算は、上記システムパラメータ N に対し、 $X^N = 1$ という関係式を用いて、演算結果が常に $N-1$ 次元以下の多項式になるように演算される。例えば、 $N=5$ の場合、多項式 $X^4 + X^2 + 1$ と多項式 $X^3 + X$ の積は、多項式と多項式の積を \times 、整数と多項式の積を \cdot とすると、 $X^5 = 1$ という関係から、

$$\begin{aligned} & (X^4 + X^2 + 1) \times (X^3 + X) \\ &= X^7 + 2 \cdot X^5 + 2 \cdot X^3 + X \\ &= X^2 \times 1 + 2 \cdot 1 + 2 \cdot X^3 + X \\ &= 2 \cdot X^3 + X^2 + X + 2 \end{aligned}$$

というように、常に $N-1$ 次元以下の多項式になるように演算される。

【0064】

(3) NTRU暗号方式の暗号化

暗号化時には、以下に述べる乱数多項式 r と公開鍵多項式 h とを用いて、平文多項式 m に多項式演算である暗号化アルゴリズム E を施して、暗号文多項式 $c = E(m, r, h)$ を生成する。ここで、 $E(m, r, h)$ は、NTRU暗号方式の暗号化アルゴリズム E に、平文多項式 m 、乱数多項式 r 及び公開鍵多項式 h を入力して得られる多項式演算の結果である。暗号化アルゴリズム E については非特許文献 2 に詳しく述べられており、ここでは説明を省略する。

【0065】

なお、NTRU暗号方式では、乱数多項式 r を生成するためのパラメータ d が予め決められており、乱数多項式 r は、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ他の係数は 0 となるように選ぶ。すなわち、乱数多項式 r は $N-1$ 次元以下の多項式であり、0 次元（定数項）から $N-1$ 次元まで、 N 個の係数があるが、この N 個の係数のうち、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつ $(N-2d)$ 個の係数は 0 となるように選ぶ。非特許文献 2 によれば、パラメータ N が $N=167$ の場合、 $d=18$ である。すなわち、18 個の係数が 1 であり、かつ 18 個の係数が -1 であり、 $131 (=167-36)$ 個の係数が 0 となるように乱数多項式 r を選ぶ。

【0066】

(4) NTRU暗号方式の復号化

復号化時には、秘密鍵多項式 f を用いて、暗号文多項式 c に多項式演算である復号アルゴリズム D を施して、復号文多項式 $m' = D(c, f)$ を生成する。ここで、 $D(c, f)$ は、NTRU暗号方式の復号アルゴリズム D に、暗号文多項式 c 、及び秘密鍵多項式 f を入力して得られる多項式演算の結果である。復号アルゴリズム D については非特許文献 2 に詳しく述べられており、ここでは説明を省略する。

【0067】

(5) NTRU暗号方式の復号エラー

ところで、このNTRU暗号方式は、復号文多項式 m' が平文多項式 m と異なる場合が発生する。この場合は、復号時に正しく平文多項式 m が得られないこと

になる。このことを復号エラーが発生するという。

【0068】

(実施の形態1)

<暗号システム1の構成>

本発明の実施の形態1における暗号システム1の全体構成を図1に示す。この暗号システム1は、NTRU暗号を用いて鍵カプセル化メカニズムによる鍵配送を行って暗号化通信を行う暗号システムであり、暗号装置110と、復号装置120とから構成され、暗号装置110と復号装置120とは、通信路130を介して接続されている。

【0069】

<暗号装置110の構成>

図2は、実施の形態1における暗号装置110の構成図である。

【0070】

暗号装置110は、図2に示すように、公開鍵入力部111、乱数生成部112、第1関数部113、暗号化部114、送信部117、共通鍵暗号部118及び共通鍵暗号文送信部119から構成される。

【0071】

(1) 公開鍵入力部111

公開鍵入力部111は、外部から復号装置120の公開鍵多項式 h を受け取り、公開鍵多項式 h を暗号化部114へ出力する。

【0072】

(2) 乱数生成部112

乱数生成部112は、乱数 s を生成して、乱数 s を第1関数部113と暗号化部114へ出力する。

【0073】

(3) 第1関数部113

第1関数部113は、乱数生成部112から乱数 s を受け取り、乱数 s の関数値 $G(s)$ を生成する。そして、関数値 $G(s)$ から共有鍵 K と乱数値 u を生成して、乱数値 u を暗号化部114へ出力し、共有鍵 K を共通鍵暗号部118へ出

力する。

【0074】

ここでは、関数 G は出力長が $2k$ ビットのハッシュ関数とし、 $G(s)$ の上位 k ビットを乱数値 u とし、 $G(s)$ の下位 k ビットを共有鍵 K とする。

【0075】

(4) 暗号化部 114

暗号化部 114 は、公開鍵入力部 111 から公開鍵多項式 h を受け取り、乱数生成部 112 から乱数 s を受け取り、第 1 関数部 113 から乱数値 u を受け取る。そして、公開鍵多項式 h と乱数値 u を用いて乱数 s の第 1 暗号文 c_1 を生成し、第 1 暗号文 c_1 を送信部 117 へ出力する。

【0076】

ここでは、第 1 暗号文 c_1 は NTRU 暗号による暗号文とし、以下のように生成する。

【0077】

まず、NTRU 暗号のパラメータ d に対し、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r を乱数値 u から一意に求まるように生成する。これは、例えば、乱数値 u を擬似乱数系列の初期値（乱数シード）として設定し、 $\{0, 1, \dots, N-1\}$ から重複しない擬似乱数 $2d$ 個を生成し、最初の d 個を擬似乱数の次元の係数を 1、残りの d 個の擬似乱数の次元の係数を -1 とし、他の次元の係数は 0 とすることで生成できる。そして、乱数 s を NTRU 暗号の暗号アルゴリズム E に適用できるように、乱数 s の下位 b ビット目の値を X^b の係数として乱数多項式 s_p を構成して、乱数多項式 s_p に変換する。すなわち、 $s = 10010$ （ビット表現）の場合、 $s_p = X^5 + X^2$ と変換する。そして、公開鍵多項式 h を使用して、乱数多項式 r を用いて乱数多項式 s_p に前記暗号アルゴリズム E を施して、暗号文多項式 $E(s_p, r, h)$ を生成し、第 1 暗号文 c_1 を $c_1 = E(s_p, r, h)$ とする。

【0078】

(5) 送信部 117

送信部 117 は、暗号化部 114 から第 1 暗号文 c_1 を受け取り、第 1 暗号文 c_1 を通信路 130 を介して復号装置 120 へ送信する。

【0079】

(6) 共通鍵暗号部 118

共通鍵暗号部 118 は、例えば DES 暗号方式のような共通鍵暗号アルゴリズム Sym を有している。

【0080】

共通鍵暗号では、暗号鍵 K を用いて、平文 m に共通鍵暗号アルゴリズム Sym を施して、暗号文 $c = Sym(m, K)$ を生成し、暗号鍵 K を用いて、暗号文 c に共通鍵暗号アルゴリズム Sym を施して、復号文 $m' = Sym(c, K)$ を生成する。ここで、暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K が同一であれば、 $m' = m$ となる。なお、共通鍵暗号及び DES 暗号方式については、非特許文献 1 に詳しく述べられているため、ここでの詳細な説明は省略する。

【0081】

共通鍵暗号部 118 は、外部から複数の平文 m_i ($1 \leq i \leq n$) を受け取り、第 1 関数部 113 から共有鍵 K を受け取り、共有鍵 K を使用して平文 m_i ($1 \leq i \leq n$) に共通鍵暗号アルゴリズム Sym を施して、共通鍵暗号文 $C_i = Sym(m_i, K)$ ($1 \leq i \leq n$) を生成する。

【0082】

そして、共通鍵暗号部 118 は、共通鍵暗号文 C_i ($1 \leq i \leq n$) を共通鍵暗号文送信部 119 へ出力する。

【0083】

(7) 共通鍵暗号文送信部 119

共通鍵暗号文送信部 119 は、共通鍵暗号化部 118 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受け取り、通信路 130 を介して復号装置 120 へ送信する。

【0084】

<暗号装置 110 の動作>

ここで、以上に述べた暗号装置 110 の動作について、図 3 に示すフローチャ

ートを用いて説明する。

【0085】

まず、公開鍵入力部111は、外部から復号装置120の公開鍵多項式 h を受け取り、公開鍵多項式 h を暗号化部114へ出力する（ステップS101）。

【0086】

次に、乱数生成部112は、乱数 s を生成して、乱数 s を第1関数部113と暗号化部114へ出力する（ステップS102）。

【0087】

次に、第1関数部113は、乱数生成部112から乱数 s を受け取り、乱数 s の関数値 $G(s)$ を生成する（ステップS103）。そして、第1関数部113は、関数値 $G(s)$ から乱数値 u と共有鍵 K を生成して、乱数値 u を暗号化部114へ出力し、共有鍵 K を共通鍵暗号部118へ出力する（ステップS104）。

【0088】

次に、暗号化部114は、公開鍵入力部111から公開鍵多項式 h を受け取り、乱数生成部112から乱数 s を受け取り、第1関数部113から乱数値 u を受け取る。そして、暗号化部114は、公開鍵多項式 h と乱数値 u を用いて乱数 s の第1暗号文 c_1 を生成し、第1暗号文 c_1 を送信部117へ出力する（ステップS105）。

【0089】

次に、送信部117は、暗号化部114から第1暗号文 c_1 を受け取り、第1暗号文 c_1 を通信路130を介して復号装置120へ送信する（ステップS106）。

【0090】

次に、共通鍵暗号部118は、外部から複数の平文 m_i ($1 \leq i \leq n$)を受け取り、第1関数部113から共有鍵 K を受け取り、共有鍵 K を使用して平文 m_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズム Sym を施して、共通鍵暗号文 $C_i = Sym(m_i, K)$ ($1 \leq i \leq n$)を生成し、共通鍵暗号文 C_i ($1 \leq i \leq n$)を共通鍵暗号文送信部119へ出力する（ステップS107）。

【0091】

次に、共通鍵暗号文送信部 119 は、共通鍵暗号化部 118 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受け取り、通信路 130 を介して復号装置 120 へ送信して処理を終了する（ステップ S108）。

【0092】

<復号装置 120 の構成>

図 4 は、実施の形態 1 における復号装置 120 の構成図である。

【0093】

復号装置 120 は、図 4 に示すように、秘密鍵入力部 121、受信部 122、復号化部 123、第 2 関数部 126、比較部 127、共通鍵復号部 128 及び共通鍵暗号文受信部 129 から構成される。

【0094】

(1) 秘密鍵入力部 121

秘密鍵入力部 121 は、外部から復号装置 120 の秘密鍵多項式 f と公開鍵多項式 h を受け取り、秘密鍵多項式 f を復号化部 123 へ出力し、公開鍵多項式 h を比較部 127 へ出力する。

【0095】

(2) 受信部 122

受信部 122 は、通信路 130 を介して暗号装置 110 から第 1 暗号文 c_1 を受け取り、第 1 暗号文 c_1 を復号化部 123 へ出力する。

【0096】

(3) 復号化部 123

復号化部 123 は、秘密鍵入力部 121 から秘密鍵多項式 f を受け取り、受信部 122 から第 1 暗号文 c_1 を受け取る。そして、秘密鍵多項式 f を用いて、第 1 暗号文 c_1 を復号して復号乱数 s' を生成し、第 1 暗号文 c_1 と復号乱数 s' を比較部 127 へ出力し、復号乱数 s' を第 2 関数部 126 へと出力する。

【0097】

ここでは、復号乱数 s' は NTRU 暗号による復号文とし、以下のように生成する。

【0098】

まず、秘密鍵多項式 f を使用して、第1暗号文 c_1 に前記復号アルゴリズム D を施して、復号乱数多項式 $s_p' = D(c_1, f)$ を生成する。そして、復号乱数多項式 s_p' は、NTRU暗号の復号文であり多項式で表現されているので、復号乱数多項式 s_p' の b 次元の項 X^b の係数を下位 b ビット目の値として復号乱数 s' を構成して、復号乱数 s' に変換する。すなわち、 $s_p' = X^5 + X^2$ の場合、 $s' = 10010$ (ビット表現) と変換する。

【0099】

(4) 第2関数部126

第2関数部126は、第1関数部113と同じ関数 G のアルゴリズムを有している。

【0100】

第2関数部126は、復号化部123から復号乱数 s' を受け取り、復号乱数 s' の関数値 $G(s')$ を生成する。そして、関数値 $G(s')$ から乱数値 u' と共有鍵 K' を生成して、乱数値 u' と共有鍵 K' を比較部127へ出力する。

【0101】

(5) 比較部127

比較部127は、秘密鍵入力部121から公開鍵多項式 h を受け取り、復号化部123から第1暗号文 c_1 と復号乱数 s' を受け取り、第2関数部126から乱数値 u' と共有鍵 K' を受け取る。そして、公開鍵多項式 h と乱数値 u' を用いて、暗号化部114と同様にして復号乱数 s' を暗号化して第1再暗号文 c_1' を生成する。そして、 $c_1' = c_1$ であれば、共有鍵 K' を共通鍵復号部128へ出力する。

【0102】

(6) 共通鍵復号部128

共通鍵復号部128は、共通鍵暗号部118が有する共通鍵暗号アルゴリズム Sym を予め有している。

【0103】

共通鍵復号部128は、比較部127から共有鍵 K' を受け取り、共通鍵暗号

文受信部 129 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受け取り、共有鍵 K' を使用して共通鍵暗号文 C_i ($1 \leq i \leq n$) に共通鍵暗号アルゴリズム Sym を施して、復号文 $m_i' = Sym(C_i, K)$ ($1 \leq i \leq n$) を生成する。

【0104】

そして、共通鍵復号部 128 は、復号文 m_i' ($1 \leq i \leq n$) を外部へ出力する。

【0105】

(7) 共通鍵暗号文受信部 129

共通鍵暗号文受信部 129 は、通信路 130 を介して暗号装置 110 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を受信し、共通鍵復号部 128 へ出力する。

【0106】

<復号装置 120 の動作>

ここで、以上に述べた復号装置 120 の動作について、図 5 に示すフローチャートを用いて説明する。

【0107】

まず、秘密鍵入力部 121 は、外部から復号装置 120 の秘密鍵多項式 f と公開鍵多項式 h を受け取り、秘密鍵多項式 f を復号化部 123 へ出力し、公開鍵多項式 h を比較部 127 へ出力する (ステップ S151)。

【0108】

次に、受信部 122 は、通信路 130 を介して暗号装置 110 から第 1 暗号文多項式 c_1 を受け取り、第 1 暗号文多項式 c_1 を復号化部 123 へ出力する (ステップ S152)。

【0109】

次に、復号化部 123 は、秘密鍵入力部 121 から秘密鍵多項式 f を受け取り、受信部 122 から第 1 暗号文 c_1 を受け取る。そして、復号化部 123 は、秘密鍵多項式 f を用いて、第 1 暗号文 c_1 を復号して復号乱数 s' を生成し、第 1 暗号文 c_1 と復号乱数 s' を比較部 127 へ出力し、復号乱数 s' を第 2 関数部 126 へ出力する (ステップ S153)。

【0110】

次に、第2関数部126は、復号化部123から復号乱数 s' を受け取り、復号乱数 s' の関数値 $G(s')$ を生成する(ステップS154)。そして、関数値 $G(s')$ から乱数値 u' と共有鍵 K' を生成して、乱数値 u' と共有鍵 K' を比較部127へ出力する(ステップS155)。

【0111】

次に、比較部127は、復号化部123から第1暗号文 c_1 を受け取り、第2関数部126から乱数値 u' と共有鍵 K' を受け取る(ステップS156)。そして、第1暗号文 c_1 が乱数値 u' を用いた復号乱数 s' の暗号文であるかどうかチェックを行い、第1暗号文 c_1 が復号乱数 s' の暗号文であれば、ステップS162へ処理を移し、等しくなければ処理を終了する(ステップS157)。そして、比較部127は、共有鍵 K' を共通鍵復号部128へ出力する(ステップS158)。

【0112】

次に、共通鍵暗号文受信部129は、通信路130を介して暗号装置110から暗号文 C_i ($1 \leq i \leq n$)を受信し、共通鍵復号部128へ出力する(ステップS159)。

【0113】

次に、共通鍵復号部128は、比較部127から共有鍵 K' を受け取り、共通鍵暗号文受信部129から共通鍵暗号文 C_i ($1 \leq i \leq n$)を受け取り、共有鍵 K' を使用して共通鍵暗号文 C_i ($1 \leq i \leq n$)に共通鍵暗号アルゴリズム Sym を施して、復号文 $m_i' = Sym(C_i, K)$ ($1 \leq i \leq n$)を生成し、復号文 m_i' ($1 \leq i \leq n$)を外部へ出力して処理を終了する(ステップS160)。

【0114】

<暗号システム1の動作検証>

以下に、実施の形態1における暗号システム1の全体の動作について説明する。

【0115】

まず、暗号装置110は、復号装置120の公開鍵多項式 h を入力とし、乱数

s を生成して、関数値 $G(s)$ から乱数値 u と共有鍵 K を導出する。そして、暗号装置 110 は、乱数 s を、公開鍵多項式 h と乱数値 u を用いて NTRU 暗号で暗号化して第 1 暗号文 c_1 を生成し、第 1 暗号文 c_1 を通信路 130 を介して復号装置 120 へ送信する。

【0116】

すなわち、この暗号装置 110 は、以下の処理を行い、第 1 暗号文 c_1 を復号装置 120 へ送信する。

【0117】

- ・乱数 s を生成する。

【0118】

- ・ $G(s)$ を生成し、 $G(s)$ から u 、 K を生成する。

【0119】

- ・公開鍵多項式 h と乱数値 u を用いて乱数 s の第 1 暗号文 c_1 を生成する。

【0120】

- ・共有鍵 K と第 1 暗号文 c_1 を出力する。

【0121】

次に、暗号装置 110 は、導出した共有鍵 K を用いて、外部から入力された平文 m_i ($1 \leq i \leq n$) を共通鍵暗号で暗号化して暗号文 C_i ($1 \leq i \leq n$) を生成し、通信路 130 を介して復号装置 120 へ送信する。

【0122】

一方、復号装置 120 は、復号装置 120 の秘密鍵多項式 f 及び公開鍵多項式 h を入力とし、通信路 130 を介して暗号装置 110 から第 1 暗号文 c_1 を受信し、第 1 暗号文 c_1 を秘密鍵多項式 f を用いて復号して復号乱数 s' を生成する。そして、復号乱数 s' の関数値 $G(s')$ から乱数値 u' と共有鍵 K' を導出する。そして、復号乱数 s' を暗号化して第 1 再暗号文 c_1' を生成し、 $c_1' = c_1$ であれば、共有鍵 K' を出力する。

【0123】

すなわち、この復号装置 120 は、以下の処理を行い、共有鍵 K' を導出する。

【0124】

- ・秘密鍵多項式 f を用いて第1暗号文 c_1 を復号して s' を生成する。

【0125】

- ・ $G(s')$ を生成し、 $G(s')$ から u' 、 K' を生成する。

【0126】

- ・公開鍵多項式 h 、乱数値 u' を用いて s' の第1再暗号文 c_1' を生成する

。

【0127】

- ・ $c_1' = c_1$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

【0128】

ここで、暗号装置 110 で用いられた公開鍵多項式 h に対応する正しい秘密鍵多項式 f が復号装置 120 で用いられれば、第1暗号文 c_1 は正しく復号されて、復号乱数 s' は $s' = s$ となり、従って、 $G(s')$ から導出される乱数値 u' は $u' = u$ となり、共有鍵 K' は $K' = K$ となる。そして、 $s' = s$ 及び $u' = u$ が成り立つので、 $c_1' = c_1$ が成り立ち、復号装置 120 は暗号装置 110 と同じ共有鍵 K を導出できることになる。

【0129】

次に、復号装置 120 は、導出した共有鍵 K' ($=K$) を用いて、通信路を介して暗号装置 110 から共通鍵暗号文 C_i ($1 \leq i \leq n$) を共通鍵暗号で復号して復号文 m_i' ($1 \leq i \leq n$) を生成して外部へ出力する。今、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' は同一なので、復号装置 120 は、正しく $m_i' = m_i$ ($1 \leq i \leq n$) を得ることができる。

【0130】

なお、復号エラーが発生した場合には、復号乱数 s' と乱数 s とは異なるので、 $G(s')$ から導出される乱数値 u' 及び共有鍵 K' はそれぞれ u 、 K とは異なる。しかし、この場合、 s' 、 u' がそれぞれ s 、 u と異なるために第1再暗号文 c_1' が第1暗号文 c_1 と異なるので、復号装置 120 は、共有鍵 K' を出力しない。

【0131】

＜実施の形態1における効果＞

RSA-KEMアルゴリズムは、暗号文Cから秘密鍵を知らなければ導出できないランダムな要素sをハッシュ関数Gに入力して共有鍵Kを導出するようにしていた。しかしながら、NTRU暗号は、鍵カプセル化メカニズムであるRSA-KEMアルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いてもランダムな要素sが導出できず、従って正しくない共有鍵K'を導出する場合があった。

【0132】

しかしながら、この暗号システム、暗号装置及び復号装置は、乱数sのハッシュ関数値G(s)から共有鍵に加えて乱数値uを生成し、復号装置が乱数値uと公開鍵多項式hを用いて復号乱数s'を再暗号化して第1再暗号文c1'を生成し、第1再暗号文c1'が第1暗号文c1と同じ値でない限り共有鍵K'を出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できるようになった。

【0133】

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0134】

(1) 用いるNTRU暗号のパラメータは $N=167$ に限定されず、他のパラメータでもよい。

【0135】

(2) 暗号化部114、復号化部123で行われるビット列と多項式との変換方法は、この方法に限られず他の変換方法でもよい。

【0136】

例えば、ビット列と多項式を1対1に対応させる関数もしくは関数値のテーブルを用いて変換してもよい。

【0137】

(3) 暗号化部114、復号化部123で用いる公開鍵暗号は、暗号化部114において、乱数 s を公開鍵と乱数値 u を用いて暗号化して第1暗号文 $c1$ を生成し、復号化部123において、第1暗号文 $c1$ を秘密鍵で復号して乱数値 s と等しい復号乱数 s' を生成できればよい。従って、暗号化部114、復号化部123で用いる公開鍵暗号は、NTRU暗号以外に、どんな公開鍵暗号でも利用できる。

【0138】

例えば、ElGamal暗号ならば、 h 、 f をそれぞれElGamal暗号の公開鍵、秘密鍵とし、暗号化部114において、乱数 s を h と u を用いて暗号化して $c1$ を生成し、復号化部123において、 $c1$ を f を用いて復号して s' を生成すればよい。

【0139】

なお、ElGamal暗号について非特許文献1に詳細に記載されているため、ここでは説明を省略する。

【0140】

(4) 第1関数部113は、関数値 $G(s)$ の上位 k ビットを乱数値 u として下位 k ビットを共有鍵 K とする以外に、関数値 $G(s)$ から乱数値 u と共有鍵 K を導出すれば他の方法でもよい。

【0141】

(5) 乱数値 u は、第1関数部113及び第2関数部126で生成される以外にも、暗号装置110と復号装置120とで同じ値を得られれば、他の生成方法でもよい。

【0142】

例えば、任意の関数 $Func$ に対し、 $u = Func(s)$ として暗号装置110と復号装置120とで同じ値を得られるようにしてもよい。すなわち、

- ・ $G(s)$ を生成し、 $G(s)$ から K を生成する。

【0143】

- ・ $Func(s)$ を生成し、 $u = Func(s)$ とする。

としてもよい。

【0144】

(6) さらに、乱数値 u は、第1関数部113及び第2関数部126で生成される以外にも、暗号装置110と復号装置120とで同じ値を得られればよい。ため、暗号装置110が乱数値 u を復号装置120bに直接送信してもよい。

【0145】

すなわち、以下のように、第1暗号文 c_1 と乱数値 u を復号装置120に送信してもよい。また、乱数値 u は暗号化して送信されてもよい。

【0146】

・ $G(s)$ を生成し、 $G(s)$ から K を生成する。

【0147】

・ 乱数値 u は、別途、暗号装置110bから120bへ送信される。

【0148】

(7) さらに、乱数値 u は、暗号装置110と復号装置120とで同じ値を得られればよい。ため、乱数値 u の部分情報を第1関数部113及び第2関数部126で生成し、乱数値 u の残りの部分情報を暗号装置110から復号装置120に直接送信してもよい。

【0149】

例えば、以下のように、第1暗号文 c_1 と乱数値 u_2 を復号装置120に送信してもよい。また、乱数値 u_2 は暗号化して送信されてもよい。

【0150】

・ $G(s)$ を生成し、 $G(s)$ から K 、 u_1 を生成する。

【0151】

・ 乱数値 u_2 は、別途、暗号装置110から120へ送信される。

【0152】

・ 乱数値 u は、 $u = u_1 \text{ xor } u_2$ から生成される。

【0153】

(8) なお、復号エラー発生により暗号装置110と復号装置120との間で異なる鍵が導出されるのを防止するため、第1再暗号文 c_1' が第1暗号文 c_1

と同じ値かどうかを検証して共有鍵 K' を出力する代わりに、暗号装置 110 が乱数 s 、乱数値 u 、共有鍵 K のいずれかのハッシュ関数値を生成し、復号装置 120 がこのハッシュ関数値を検証して共有鍵 K' を出力するか否かを決定してもよい。

【0154】

例えば、暗号装置 110 が乱数 s のハッシュ関数値を生成し、復号装置 120 がこのハッシュ関数値を検証する場合、暗号装置 110 は、図 6 に示すように、

- ・第 1 関数部 113 が、 $G(s)$ を生成し、 $G(s)$ から K を生成する。

【0155】

・暗号化部 114 が、公開鍵多項式 h を用いて乱数 s の第 1 暗号文 c_1 と、ハッシュ関数値 $H(s)$ を生成する。

【0156】

・送信部 117 が、第 1 暗号文 c_1 とハッシュ関数値 $H(s)$ を送信する。
という処理を行い、復号装置 120 は、図 7 に示すように、

- ・受信部 122 が、第 1 暗号文 c_1 とハッシュ関数値 $H(s)$ を受信する。

【0157】

・復号化部 123 が、秘密鍵多項式 f を用いて第 1 暗号文 c_1 を復号して s' を生成する。

【0158】

・第 2 関数部 126 が、 $G(s')$ を生成し、 $G(s')$ から K' を生成する。
。

【0159】

・比較部 127 が $H(s')$ を生成し、 $H(s') = H(s)$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。
という処理を行ってもよい。

【0160】

さらに、この場合、安全性を高めるために、特許文献 1 に開示されている方法を用いて、乱数 s に付加情報を附したものを暗号化して第 1 暗号文 c_1 を生成してもよい。すなわち、図 6 において、暗号化部 114 が付加情報 R_a を生成し、

s と R a のビット結合 $s || R a$ の値を暗号化して第 1 暗号文 c_1 を生成し、図 7 において、復号化部 123 が、第 1 暗号文 c_1 を復号して $s' || R a'$ を生成し、 $R a'$ を除去して復号乱数 s' を生成してもよい。なお、特許文献 1 に開示されている通り、 $s || R a$ の値の代わりに、 s と $R a$ の可逆変換 $F(s, R a)$ の値を用いてもよい。

【0161】

(9) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0162】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、CD-ROM、DVD-ROM、DVD-RAM等、に記録したものとしてもよい。

【0163】

(10) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0164】

(実施の形態 2)

本発明の実施の形態 2 における暗号システム 2 は、暗号システム 1 を基本にして変形した暗号システムであり、関数値 $G(s)$ から乱数値 u と共有鍵 K の他にさらに検証値 a を生成する点と、暗号装置が、乱数 s を暗号化した第 1 暗号文 c_1 を生成して送信する代わりに、検証値 a を暗号化した第 1 暗号文 c_1 と、乱数 s を検証値 a に基づいて暗号化して第 2 暗号文 c_2 とを生成して送信する点が暗号システム 1 と異なる。

【0165】

以下、暗号システム 2 について、上記差異点を中心に詳しく説明する。

【0166】

<暗号システム 2 の構成>

本発明の実施の形態2における暗号システム2の全体構成を図8に示す。この暗号システム2は、NTRU暗号を用いて鍵配送を行う暗号システムであり、暗号装置110bと、復号装置120bとから構成され、暗号装置110bと復号装置120bとは、通信路130を介して接続されている。

【0167】

＜暗号装置110bの構成＞

図9は、実施の形態2における暗号装置110bの構成図である。

【0168】

暗号装置110bは、図9に示すように、公開鍵入力部111、乱数生成部112b、第1関数部113b、暗号化部114b、乱数マスク部116、送信部117b、共通鍵暗号部118及び共通鍵暗号文送信部119から構成される。

【0169】

以下、暗号システム1と異なる乱数生成部112b、第1関数部113b、暗号化部114b、乱数マスク部116及び送信部117bについてその構成と動作を説明する。

【0170】

(1) 乱数生成部112b

乱数生成部112bは、乱数 s を生成して、乱数 s を第1関数部113bと乱数マスク部116へ出力する。

【0171】

(2) 第1関数部113b

第1関数部113bは、乱数生成部112bから乱数 s を受け取り、乱数 s の関数値 $G(s)$ を生成する。そして、関数値 $G(s)$ から検証値 a と共有鍵 K と乱数値 u を生成して、検証値 a と乱数値 u を暗号化部114bへ出力し、共有鍵 K を共通鍵暗号部118へ出力し、検証値 a を乱数マスク部116へ出力する。

【0172】

ここでは、関数 G は出力長が $3k$ ビットのハッシュ関数とし、 $G(s)$ の上位 k ビットを検証値 a とし、 $G(s)$ の中間の k ビットを共有鍵 K し、 $G(s)$ の下位 k ビットを乱数値 u とする。

【0173】

(3) 暗号化部 114b

暗号化部 114b は、公開鍵入力部 111 から公開鍵多項式 h を受け取り、第 1 関数部 113b から検証値 a と乱数値 u を受け取る。そして、公開鍵多項式 h と乱数値 u を用いて検証値 a の第 1 暗号文 c_1 を生成し、第 1 暗号文 c_1 を送信部 117b へ出力する。

【0174】

ここでは、第 1 暗号文 c_1 は NTRU 暗号による暗号文とし、以下のように生成する。

【0175】

まず、NTRU 暗号のパラメータ d に対し、 d 個の係数が 1 であり、かつ d 個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式 r を乱数値 u から一意に求まるように生成する。これは、例えば、乱数値 u を擬似乱数系列の初期値（乱数シード）として設定し、 $\{0, 1, \dots, N-1\}$ から重複しない擬似乱数 $2d$ 個を生成し、最初の d 個を擬似乱数の次元の係数を 1、残りの d 個の擬似乱数の次元の係数を -1 とし、他の次元の係数は 0 とすることで生成できる。そして、検証値 a を NTRU 暗号の暗号アルゴリズム E に適用できるように、検証値 a の下位 b ビット目の値を X^b の係数として検証値多項式 a_p を構成して、検証値多項式 a_p に変換する。すなわち、 $a = 10010$ （ビット表現）の場合、 $a_p = X^5 + X^2$ と変換する。そして、公開鍵多項式 h を使用して、乱数多項式 r を用いて検証値多項式 a_p に前記暗号アルゴリズム E を施して、暗号文多項式 $E(a_p, r, h)$ を生成し、第 1 暗号文 c_1 を $c_1 = E(a_p, r, h)$ とする。

【0176】

(4) 乱数マスク部 116

乱数マスク部 116 は、乱数生成部 112b から乱数 s を受け取り、第 1 関数部 113b から検証値 a を受け取る。そして、第 2 暗号文 c_2 として $c_2 = s \oplus a$ を生成し、第 2 暗号文 c_2 を送信部 117b へ出力する。ここで、 \oplus は排他的論理和演算を表す。

【0177】**(5) 送信部 117b**

送信部 117b は、暗号化部 114b から第 1 暗号文 c_1 を受け取り、乱数マスク部 116 から第 2 暗号文 c_2 を受け取り、第 1 暗号文 c_1 と第 2 暗号文 c_2 を通信路 130 を介して復号装置 120b へ送信する。

【0178】**< 復号装置 120b の構成 >**

図 10 は、実施の形態 2 における復号装置 120b の構成図である。

【0179】

復号装置 120b は、図 10 に示すように、秘密鍵入力部 121、受信部 122b、復号化部 123b、乱数マスク除去部 125、第 2 関数部 126b、比較部 127b、共通鍵復号部 128 及び共通鍵暗号文受信部 129 から構成される。

【0180】

以下、暗号システム 1 と異なる受信部 122b、復号化部 123b、乱数マスク除去部 125、第 2 関数部 126b 及び比較部 127b についてその構成と動作を説明する。

【0181】**(1) 受信部 122b**

受信部 122b は、通信路 130 を介して暗号装置 110b から第 1 暗号文 c_1 と第 2 暗号文 c_2 を受け取り、第 1 暗号文 c_1 を復号化部 123b へ出力し、第 2 暗号文 c_2 を乱数マスク除去部 125 へ出力する。

【0182】**(2) 復号化部 123b**

復号化部 123b は、秘密鍵入力部 121 から秘密鍵多項式 f を受け取り、受信部 122b から第 1 暗号文 c_1 を受け取る。そして、秘密鍵多項式 f を用いて、第 1 暗号文 c_1 を復号して復号検証値 a' を生成し、復号検証値 a' を乱数マスク除去部 125 へ出力して、第 1 暗号文 c_1 を比較部 127b に出力する。

【0183】

ここでは、復号検証値 a' は NTRU 暗号による復号文とし、以下のように生成する。

【0184】

まず、秘密鍵多項式 f を使用して、第 1 暗号文 c_1 に前記復号アルゴリズム D を施して、復号検証値多項式 $a_p' = D(c_1, f)$ を生成する。そして、復号検証値多項式 a_p' は、NTRU 暗号の復号文であり多項式で表現されているので、復号検証値多項式 a_p' の b 次元の項 X^b の係数を下位 b ビット目の値として復号検証値 a' を構成して、復号検証値 a' に変換する。すなわち、 $a_p' = X^5 + X^2$ の場合、 $a' = 10010$ (ビット表現) と変換する。

【0185】

(3) 乱数マスク除去部 125

乱数マスク除去部 125 は、受信部 122b から第 2 暗号文 c_2 を受け取り、復号化部 123b から復号検証値 a' を受け取る。そして、復号乱数 s' として、 $s' = c_2 \text{ xor } a'$ を生成し、復号乱数 s' を第 2 関数部 126b へ出力する。

【0186】

(4) 第 2 関数部 126b

第 2 関数部 126b は、第 1 関数部 113b と同じ関数 G のアルゴリズムを有している。

【0187】

第 2 関数部 126b は、乱数マスク除去部 125 から復号乱数 s' を受け取り、復号乱数 s' の関数値 $G(s')$ を生成する。そして、第 1 関数部 113b と同様にして、関数値 $G(s')$ から検証値 a'' と共有鍵 K' と乱数値 u' を生成して、検証値 a'' と共有鍵 K' と乱数値 u' を比較部 127b へ出力する。

【0188】

(5) 比較部 127b

比較部 127b は、秘密鍵入力部 121 から公開鍵多項式 h を受け取り、復号化部 123b から第 1 暗号文 c_1 を受け取り、第 2 関数部 126b から検証値 a'' と共有鍵 K' と乱数値 u' を受け取る。そして、公開鍵多項式 h と乱数値 u

’を用いて、暗号化部114bと同様にして検証値 a' を暗号化して第1再暗号文 $c1'$ を生成する。そして、 $c1' = c1$ であれば、共有鍵 K' を共通鍵暗号部128へ出力する。

【0189】

<暗号システム2の動作検証>

以下に、実施の形態2における暗号システム2の全体の動作について説明する。

【0190】

まず、暗号装置110bは、復号装置120bの公開鍵多項式 h を入力とし、乱数 s を生成して、関数値 $G(s)$ から検証値 a 、共有鍵 K 及び乱数値 u を導出する。そして、暗号装置110bは、検証値 a を、公開鍵多項式 h 及び乱数値 u を用いてNTRU暗号で暗号化して第1暗号文 $c1$ を生成し、検証値 a に基づき乱数 s を暗号化して第2暗号文 $c2 = s \text{ xor } a$ を生成する。そして、暗号装置110bは、第1暗号文 $c1$ と第2暗号文 $c2$ を通信路130を介して復号装置120bへ送信する。

【0191】

すなわち、この暗号装置110bは、以下の処理を行い、暗号文 $C = (c1, c2)$ を復号装置120bへ送信する。

【0192】

・乱数 s を生成する。

【0193】

・ $G(s)$ を生成し、 $G(s)$ から a 、 K 、 u を生成する。

【0194】

・公開鍵多項式 h 、乱数値 u を用いて検証値 a の第1暗号文 $c1$ を生成する。

【0195】

・ $c2 = s \text{ xor } a$ を生成する。

【0196】

・共有鍵 K と暗号文 $C = (c1, c2)$ を出力する。

【0197】

次に、暗号装置 110b は、導出した共有鍵 K を用いて、外部から入力された平文 m_i ($1 \leq i \leq n$) を共通鍵暗号で暗号化して暗号文 C_i ($1 \leq i \leq n$) を生成し、通信路 130 を介して復号装置 120b へ送信する。

【0198】

一方、復号装置 120b は、復号装置 120b の秘密鍵多項式 f 及び公開鍵多項式 h を入力とし、通信路 130 を介して暗号装置 110b から第 1 暗号文 c_1 と第 2 暗号文 c_2 を受信し、第 1 暗号文 c_1 を秘密鍵多項式 f を用いて復号して復号検証値 a' を生成する。そして、復号検証値 a' に基づき第 2 暗号文 c_2 を復号して、復号乱数 $s' = c_2 \text{ xor } a'$ を生成する。そして、復号装置 120b は、復号乱数 s' の関数値 $G(s')$ から検証値 a'' 、共有鍵 K' 及び乱数値 u' を導出する。そして、検証値 a'' を暗号化して第 1 再暗号文 c_1' を生成し、 $c_1' = c_1$ であれば、共有鍵 K' を出力する。

【0199】

すなわち、この復号装置 120b は、以下の処理を行い、共有鍵 K' を導出する。

【0200】

・秘密鍵多項式 f を用いて第 1 暗号文 c_1 を復号して a' を生成する。

【0201】

・ $s' = c_2 \text{ xor } a'$ を生成する。

【0202】

・ $G(s')$ を生成し、 $G(s')$ から a'' 、 K' 、 u' を生成する。

【0203】

・公開鍵多項式 h 、乱数値 u' を用いて a'' の第 1 再暗号文 c_1' を生成する。

【0204】

・ $c_1' = c_1$ が成立するかどうかチェックする。成立すれば共有鍵 K' を出力する。

【0205】

ここで、暗号装置 110b で用いられた公開鍵多項式 h に対応する正しい秘密

鍵多項式 f が復号装置 120b で用いられれば、第 1 暗号文 c_1 は正しく復号されて、復号検証値 a' は $a' = a$ となり、第 2 暗号文 c_2 と a' から生成される復号乱数 s' は $s' = s$ となる。従って、 $G(s')$ から導出される検証値 a'' は $a'' = a$ となり、共有鍵 K' は $K' = K$ となり、乱数値 u' は $u' = u$ となる。そして、 $a'' = a$ 及び $u' = u$ が成り立つので、 $c_1' = c_1$ が成り立ち、復号装置 120b は暗号装置 110b と同じ共有鍵 K を導出できることになる。

【0206】

次に、復号装置 120b は、導出した共有鍵 K' ($=K$) を用いて、通信路を介して暗号装置 110b から共通鍵暗号文 C_i ($1 \leq i \leq n$) を共通鍵暗号で復号して復号文 m_i' ($1 \leq i \leq n$) を生成して外部へ出力する。今、共通鍵暗号文生成時に用いた暗号鍵 K と復号文生成時に用いる暗号鍵 K' は同一なので、復号装置 120b は、正しく $m_i' = m_i$ ($1 \leq i \leq n$) を得ることができる。

なお、復号エラーが発生した場合には、復号検証値 a' と検証値 a とは異なるので、第 2 暗号文 c_2 から得られる復号乱数 s' は s と異なる。従って、 $G(s')$ から導出される乱数値 u' 及び共有鍵 K' はそれぞれ u 、 K とは異なる。しかし、この場合、 a' 、 u' がそれぞれ s 、 u と異なるために第 1 再暗号文 c_1' が第 1 暗号文 c_1 と異なるので、復号装置 120b は、共有鍵 K' を出力しない。

【0207】

<実施の形態 2 における効果>

RSA-KEM アルゴリズムは、暗号文 C から秘密鍵を知らなければ導出できないランダムな要素 s をハッシュ関数 G に入力して共有鍵 K を導出するようにしていた。しかしながら、NTRU 暗号は、鍵カプセル化メカニズムである RSA-KEM アルゴリズムを適用して共有鍵の配送を行おうとすると、復号エラーが発生する場合があるため、秘密鍵を用いてもランダムな要素 s が導出できず、従って正しくない共有鍵 K' を導出する場合があった。

【0208】

しかしながら、この暗号システム、暗号装置及び復号装置は、乱数 s のハッシュ関数値 $G(s)$ から共有鍵に加えて検証値 a と乱数値 u を生成し、復号装置が乱数値 u と公開鍵多項式 h を用いて復号検証値 a' を再暗号化して第 1 再暗号文 c_1' を生成し、第 1 再暗号文 c_1' が第 1 暗号文 c_1 と同じ値でない限り共有鍵 K を出力しないようにしたので、復号エラーが発生した場合、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できるようになった。

【0209】

<変形例>

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。実施の形態 1 におけるのと同様の変形を施すことができるのはもちろんであるが、以下のような場合も本発明に含まれる。

【0210】

(1) 暗号化部 114b で行われる乱数値 u から乱数多項式 r への変換方法は、この方法に限られず u から r が一意に求まれば他の変換方法でもよい。例えば、乱数値 u を多項式に対応させる関数もしくは関数値テーブルを用いて変換してもよい。

【0211】

(2) 暗号化部 114b、復号化部 123b で用いる公開鍵暗号は、暗号化部 114b において、検証値 a を公開鍵と乱数値 u を用いて暗号化して第 1 暗号文 c_1 を生成し、復号化部 123b において、第 1 暗号文 c_1 を秘密鍵で復号して、検証値 a と等しい復号検証値 a' を生成できればよい。従って、暗号化部 114b、復号化部 123b で用いる公開鍵暗号は、NTRU 暗号以外に、乱数を用いる公開鍵暗号ならばどんな暗号でも利用できる。

【0212】

例えば、ElGamal 暗号ならば、 h 、 f をそれぞれ ElGamal 暗号の公開鍵、秘密鍵とし、暗号化部 114b において、 a を h と乱数値 u を用いて暗号化して c_1 を生成し、復号化部 123b において、 c_1 を f を用いて復号して a' を生成すればよい。

【0213】

(3) 乱数値 u は、第1関数部 113 b 及び第2関数部 126 b で生成される以外にも、暗号装置 110 b と復号装置 120 b とで同じ値を得られれば、他の生成方法でもよい。

【0214】

例えば、任意の関数 $Func$ に対し、 $u = Func(s)$ として暗号装置 110 b と復号装置 120 b とで同じ値を得られるようにしてもよい。すなわち、

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。

【0215】

・ $Func(s)$ を生成し、 $u = Func(s)$ とする。
としてもよい。

【0216】

(4) さらに、乱数値 u は、第1関数部 113 b 及び第2関数部 126 b で生成される以外にも、暗号装置 110 b と復号装置 120 b とで同じ値を得られればよい。また、暗号装置 110 b が乱数値 u を復号装置 120 b に直接送信してもよい。

【0217】

すなわち、以下のように、暗号文 C と乱数値 u を復号装置 120 b に送信してもよい。また、乱数値 u は暗号化して送信されてもよい。

【0218】

- ・ $G(s)$ を生成し、 $G(s)$ から a 、 K を生成する。

【0219】

- ・ 乱数値 u は、別途、暗号装置 110 b から 120 b へ送信される。

【0220】

(5) さらに、乱数値 u は、暗号装置 110 b と復号装置 120 b とで同じ値を得られればよい。また、乱数値 u の部分情報を第1関数部 113 b 及び第2関数部 126 b で生成し、乱数値 u の残りの部分情報を暗号装置 110 b から復号装置 120 b に直接送信してもよい。

【0221】

例えば、以下のように、暗号文Cと乱数値u2を復号装置120bに送信してもよい。また、乱数値u2は暗号化して送信されてもよい。

【0222】

- ・G(s)を生成し、G(s)からa、K、u1を生成する。

【0223】

- ・乱数値u2は、別途、暗号装置110bから120bへ送信される。

【0224】

- ・乱数値uは、 $u = u1 \text{ xor } u2$ から生成される。

【0225】

(6) 復号装置120bは、第1暗号文c1が第2関数部126bで得られる検証値a'の暗号文かどうかチェックを行い、c1がa'の暗号文であるときに共有鍵K'を用いて共通鍵暗号文Ciを復号しているが、このチェックは、第1暗号文c1が復号検証値a'の暗号文かどうかのチェックでもよい。

【0226】

(7) また、復号装置120bは、第1暗号文c1が第2関数部126bで得られる検証値a'の暗号文かどうかチェックを行い、c1がa'の暗号文であるときに共有鍵K'を用いて共通鍵暗号文Ciを復号しているが、このチェックは、比較部127bにおいて、復号化部123bが復号したa'の値と第2関数部126bが生成したa'の値が等しいかどうかのチェックでもよい。

【0227】

(8) なお、復号エラー発生により暗号装置110bと復号装置120bとの間で異なる鍵が導出されるのを防止するため、第1再暗号文c1'が第1暗号文c1と同じ値かどうかを検証して共有鍵K'を出力する代わりに、暗号装置110bが乱数s、検証値a、乱数値u、共有鍵Kのいずれかのハッシュ関数値を生成し、復号装置120bがこのハッシュ関数値を検証して共有鍵K'を出力するか否かを決定してもよいし、安全性を高めるために、特許文献1に開示されている方法を用いてもよい。すなわち、実施の形態1の変形例(8)を適用してもよい。

【0228】

(9) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0229】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、CD-ROM、DVD-ROM、DVD-RAM等、に記録したものとしてもよい。

【0230】

(10) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0231】

【発明の効果】

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、NTRU暗号を適用できる新しい鍵カプセル化メカニズムを構成することで、暗号装置と復号装置との間で異なる鍵が導出されるのを防止でき、鍵カプセル化メカニズムにより導出される鍵を用いた送信装置から受信装置への確実な暗号化通信ができるようになった。

【0232】

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価値は大きい。

【図面の簡単な説明】

【図1】

本発明の実施の形態1における暗号システム1の構成を示す図

【図2】

本発明の実施の形態1における暗号装置110の構成を示す図

【図3】

本発明の実施の形態1における暗号装置110の処理の流れ図

【図4】

本発明の実施の形態 1 における復号装置 1 2 0 の構成を示す図

【図 5】

本発明の実施の形態 1 における復号装置 1 2 0 の処理の流れ図

【図 6】

本発明の実施の形態 1 における暗号装置 1 1 0 の変形例の構成を示す図

【図 7】

本発明の実施の形態 1 における復号装置 1 2 0 の変形例の構成を示す図

【図 8】

本発明の実施の形態 2 における暗号システム 2 の構成を示す図

【図 9】

本発明の実施の形態 2 における暗号装置 1 1 0 b の構成を示す図

【図 1 0】

本発明の実施の形態 2 における復号装置 1 2 0 b の構成を示す図

【符号の説明】

- 1, 2 暗号システム
- 1 1 0, 1 1 0 a 暗号装置
- 1 1 1 公開鍵入力部
- 1 1 2, 1 1 2 b 乱数生成部
- 1 1 3, 1 1 3 b 第 1 関数部
- 1 1 4, 1 1 4 b 暗号化部
- 1 1 6 乱数マスク部
- 1 1 7, 1 1 7 b 送信部
- 1 1 8 共通鍵暗号部
- 1 1 9 共通鍵暗号文送信部
- 1 2 0, 1 2 0 b 復号装置
- 1 2 1 秘密鍵入力部
- 1 2 2, 1 2 2 b 受信部
- 1 2 3, 1 2 3 b 復号化部
- 1 2 5 乱数マスク除去部

1 2 6, 1 2 6 b 第 2 関数部

1 2 7, 1 2 7 b 比較部

1 2 8 共通鍵復号部

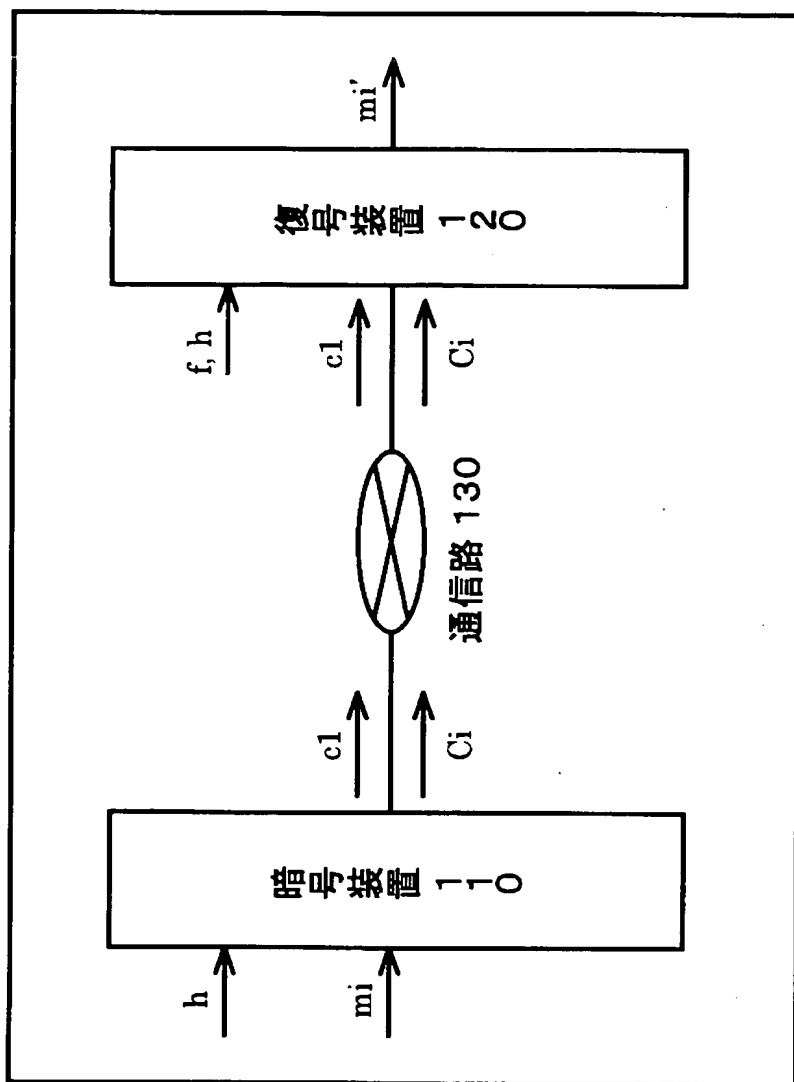
1 2 9 共通鍵暗号文受信部

1 3 0 通信路

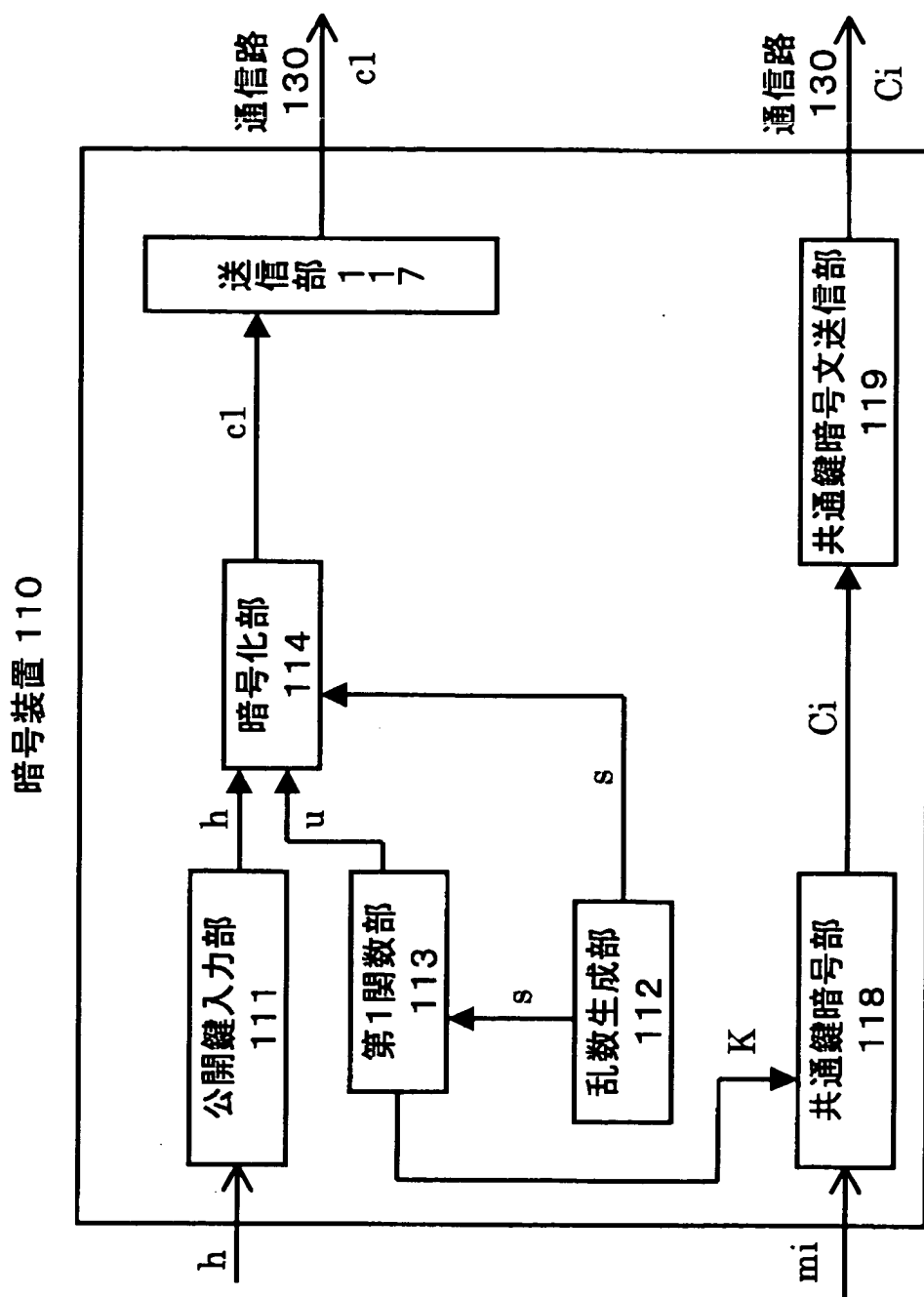
【書類名】 図面

【図 1】

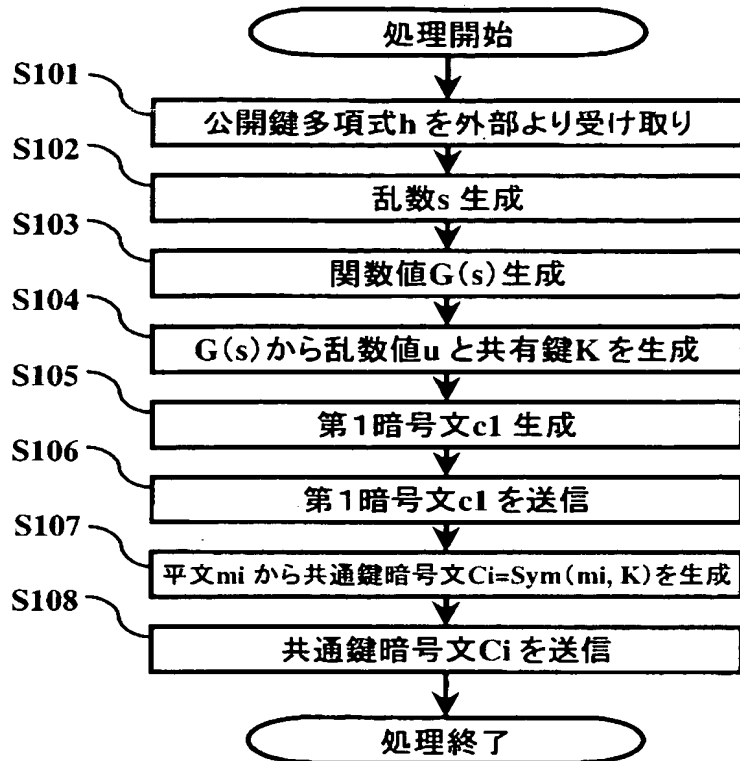
暗号システム 1



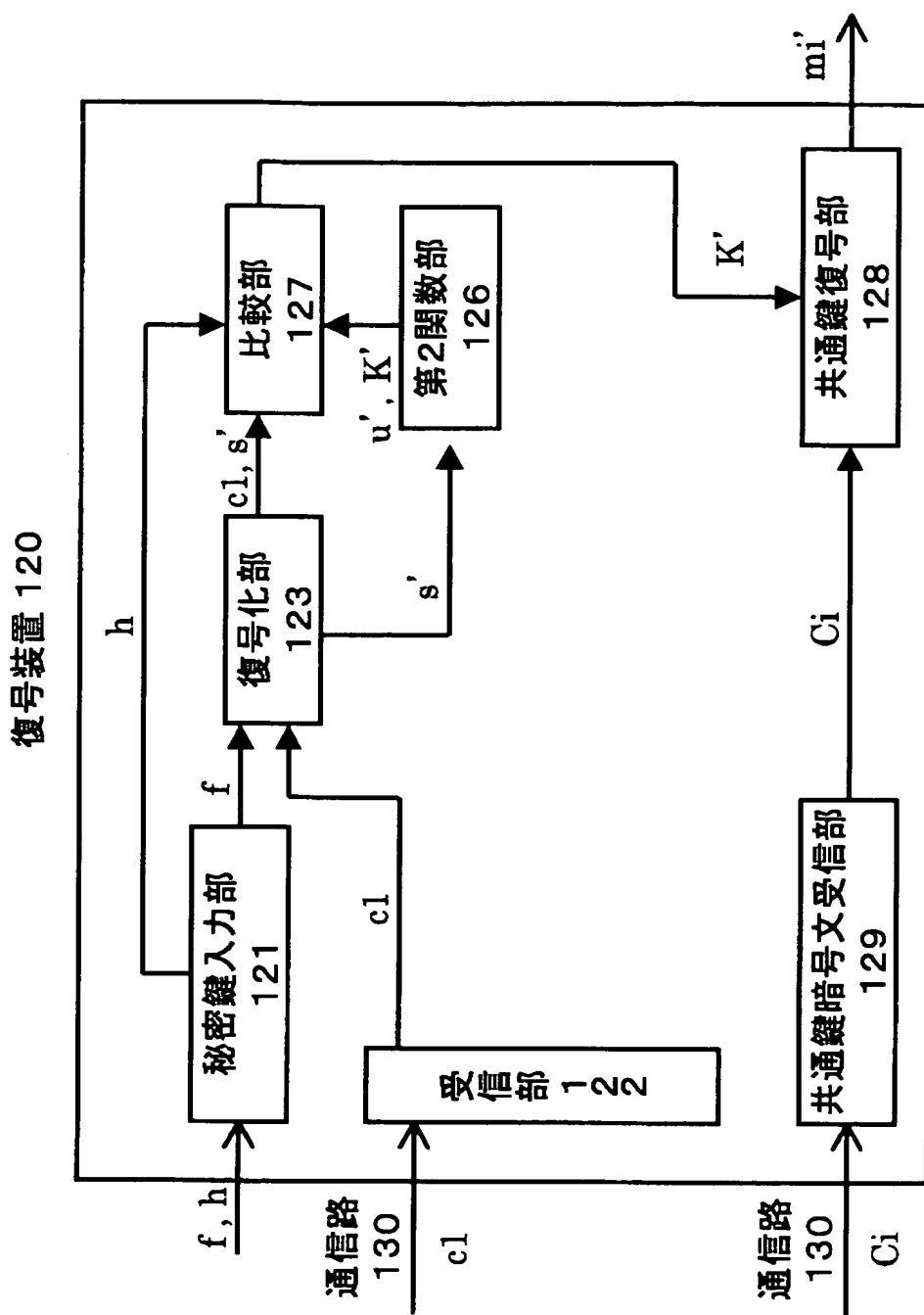
【図 2】



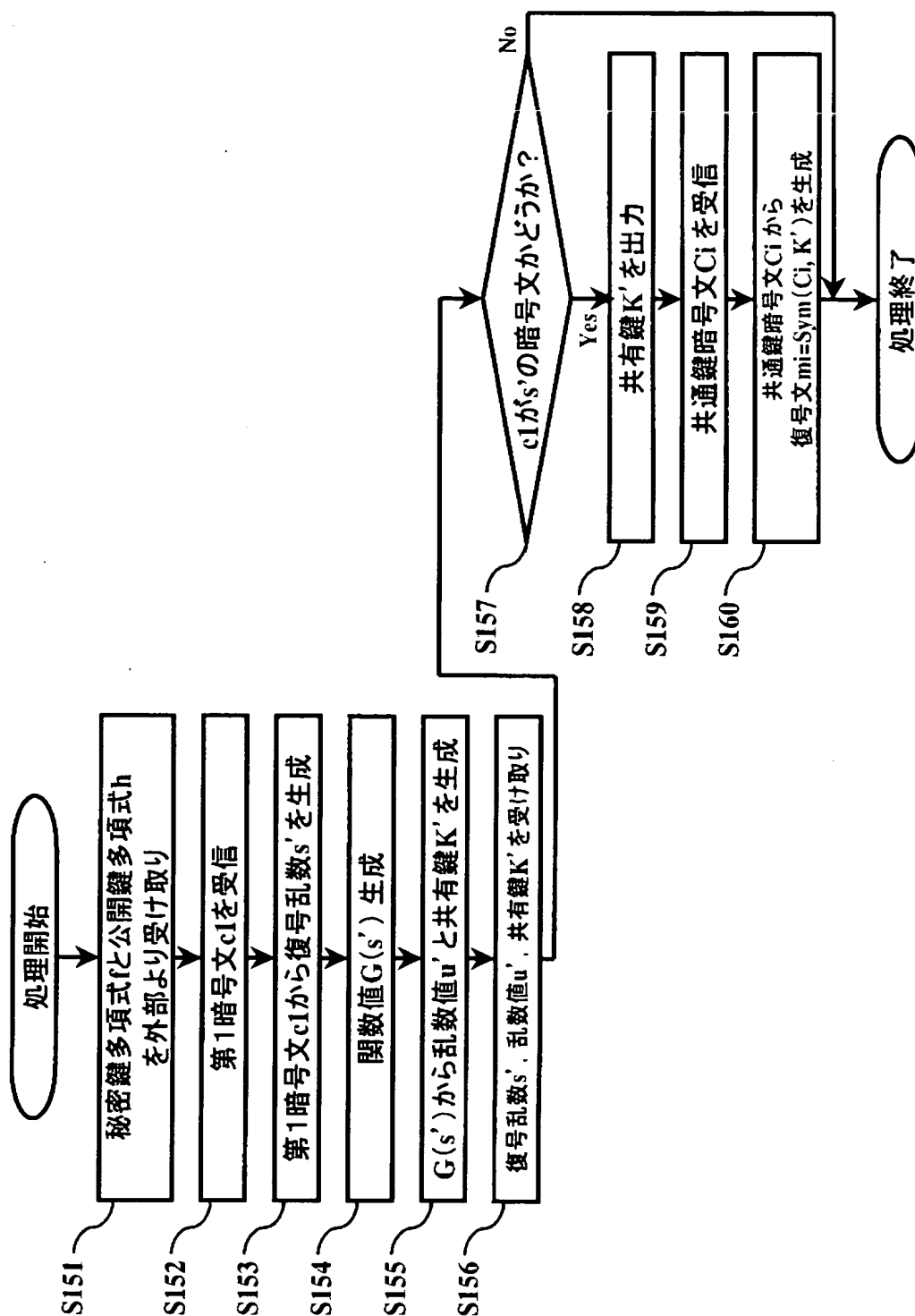
【図 3】



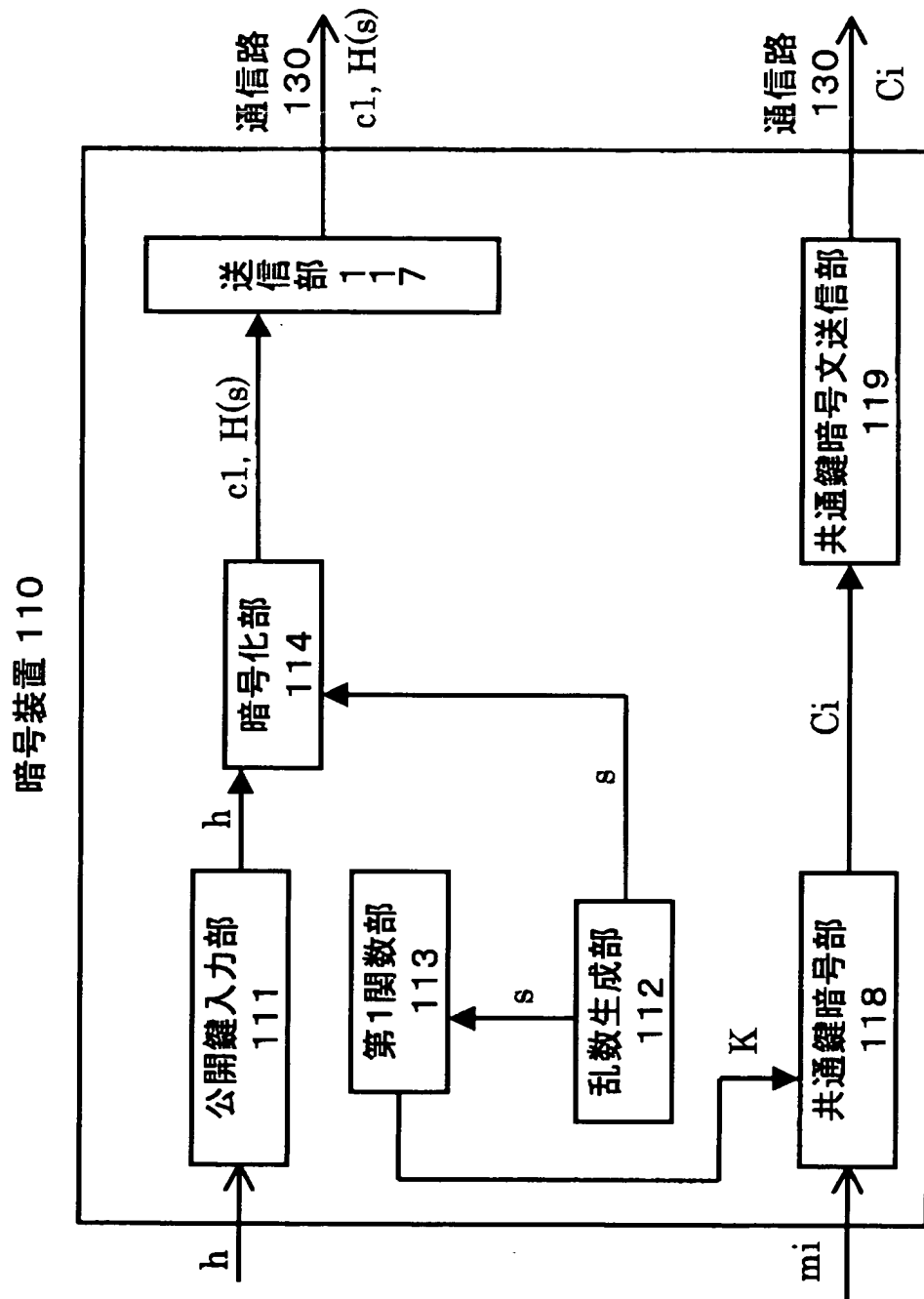
【図 4】



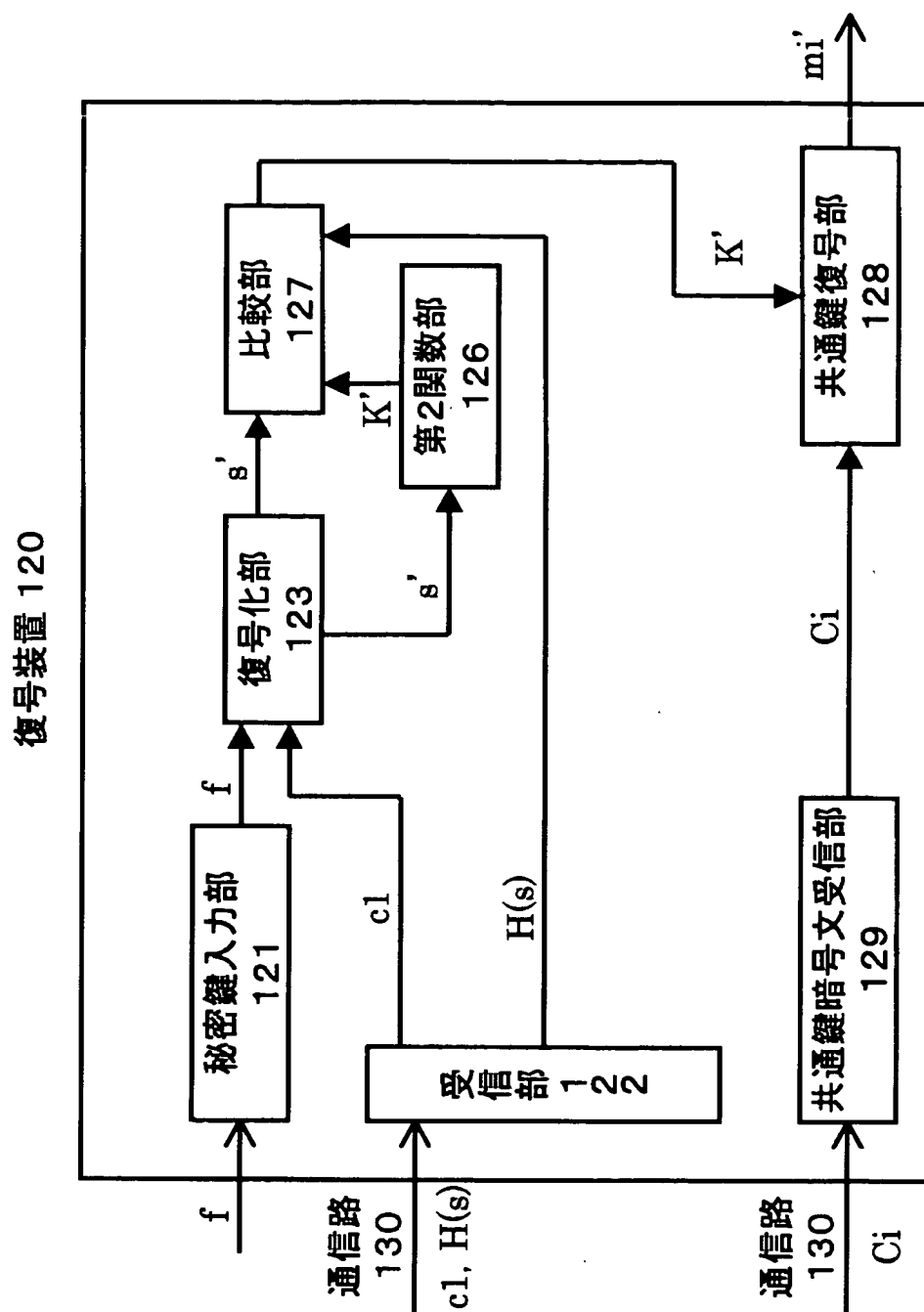
【図 5】



【図 6】

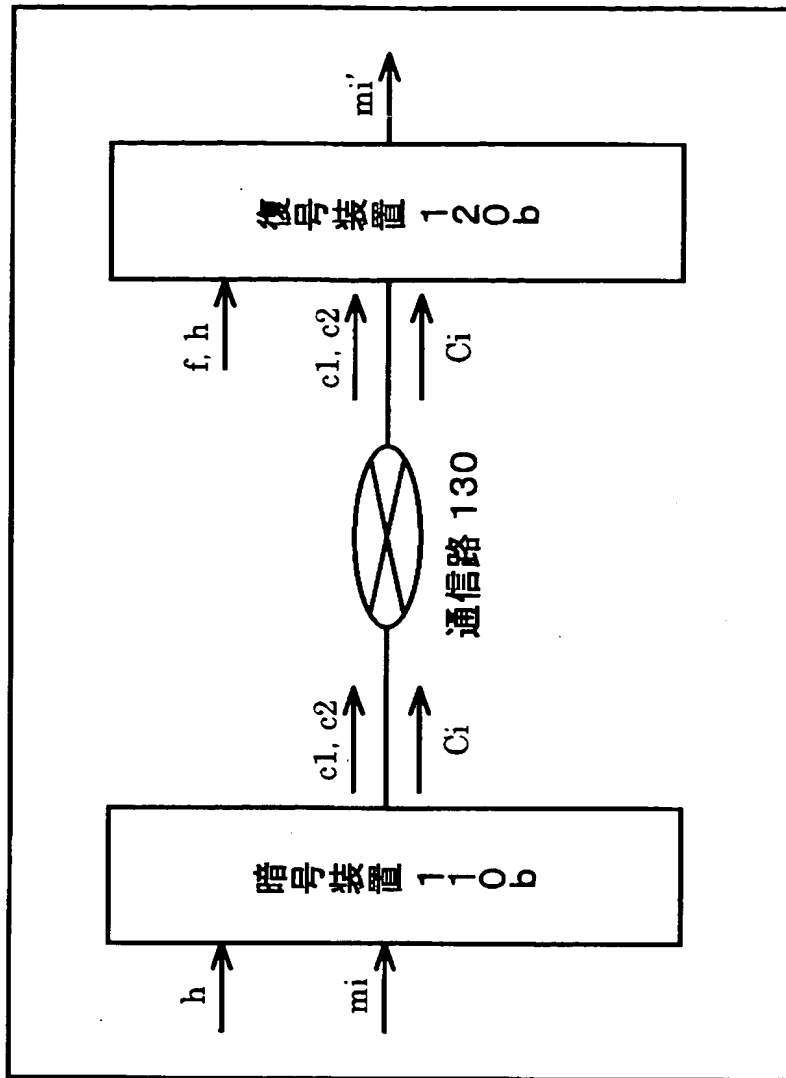


【図 7】

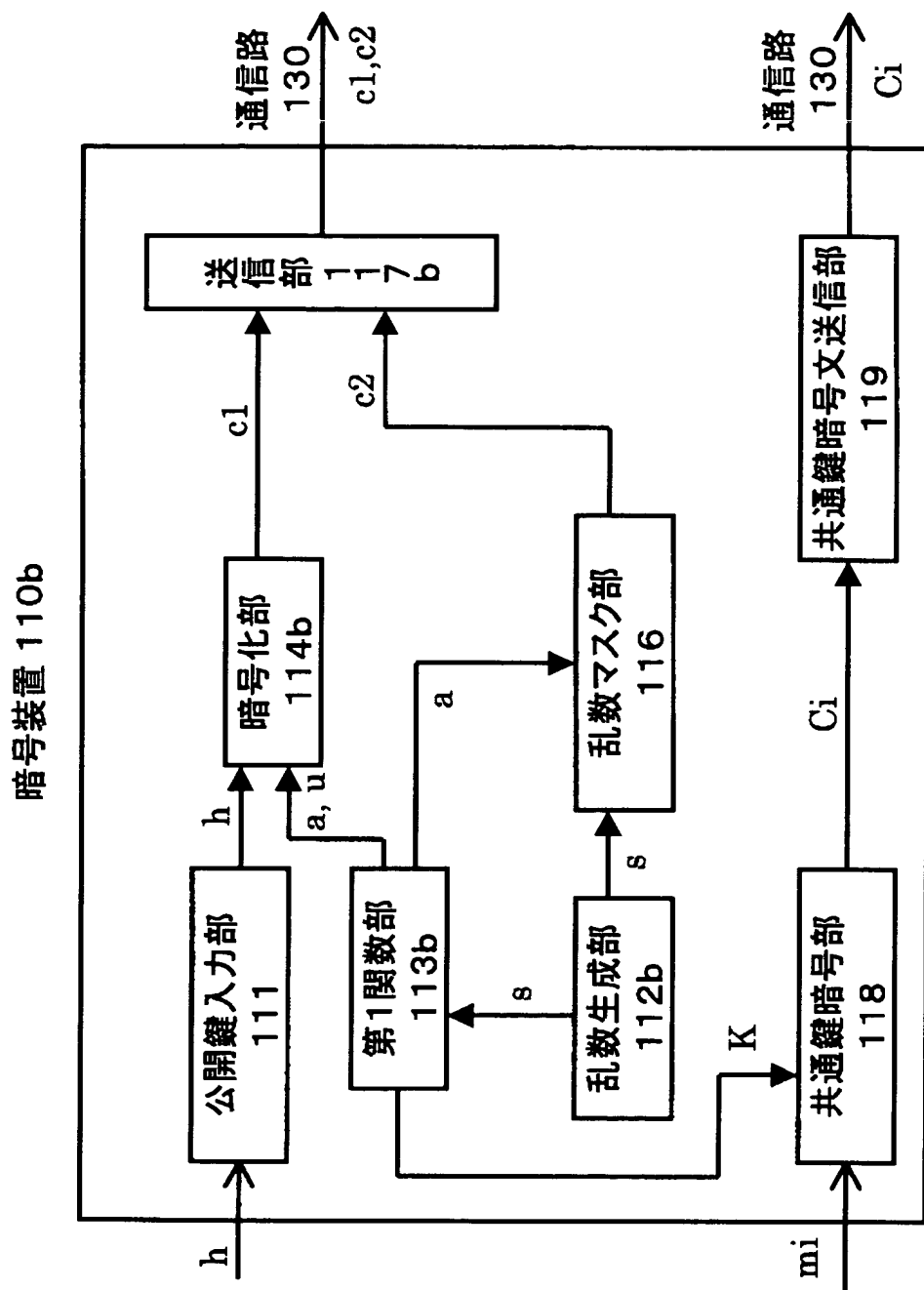


【図 8】

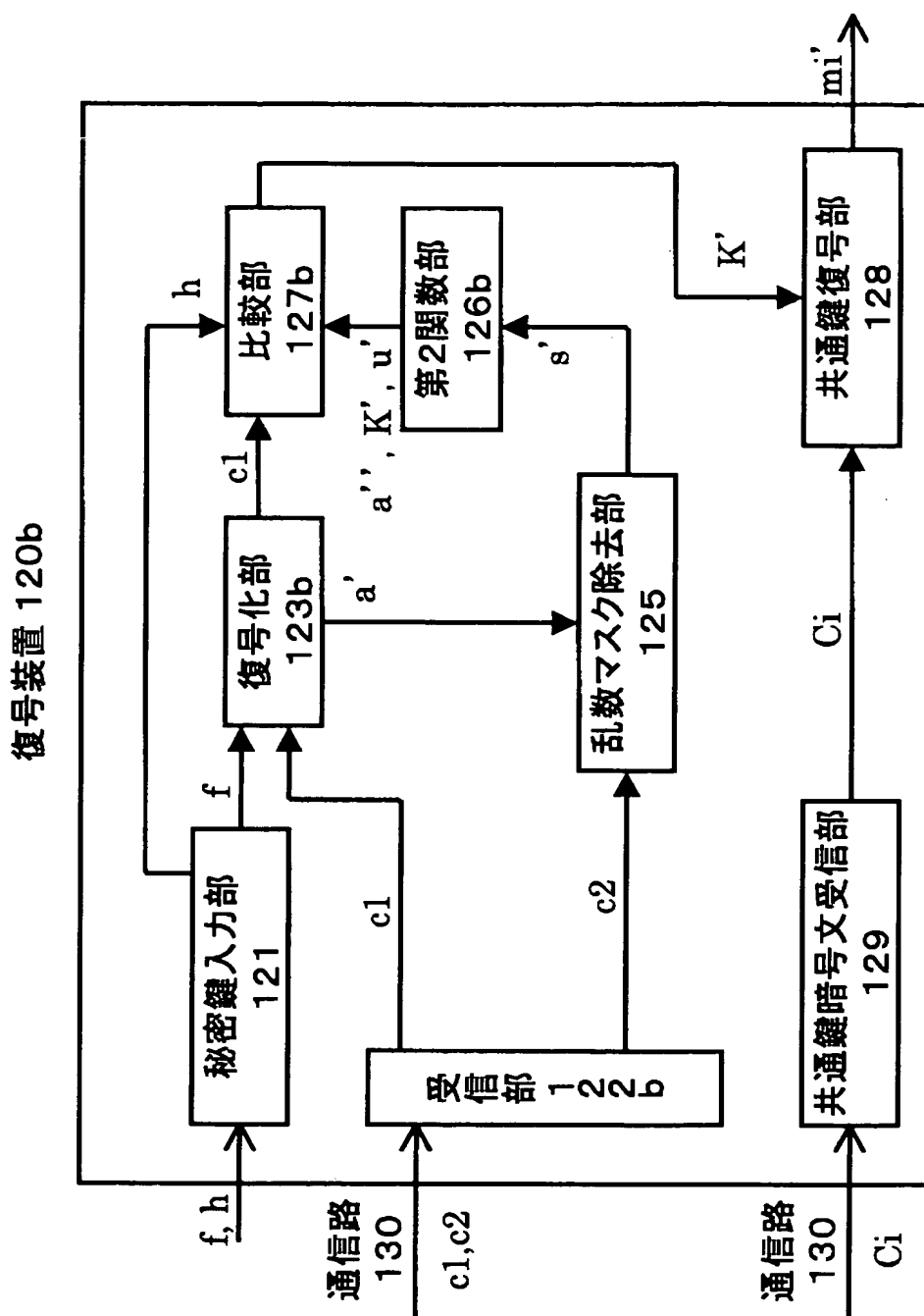
暗号システム 2



【図 9】



【図 10】



【書類名】 要約書**【要約】**

【課題】 NTRU暗号を用いて新しい鍵カプセル化メカニズムを構成し、暗号装置と復号装置との間で異なる鍵が導出されるのを防止できる暗号システム、暗号装置、復号装置を提供することを第1の目的とする。

【解決手段】 本発明は、秘密数データを生成する秘密数データ生成手段と、前記秘密数データを所定の処理に基づいて乱数データと前記共有鍵データに変換する共有鍵導出手段と、前記秘密数データを前記公開鍵データと前記乱数データに基づいて暗号化して暗号化共有鍵データを生成する第1の暗号化手段とを備えることを特徴とする。

【選択図】 図2

特願 2 0 0 2 - 3 5 1 0 6 3

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社